2023 City of Boston Annual Surveillance Technology Report

Department: Boston Housing Authority
Surveillance Technology: Body Worn Cameras

1. **Description: A description of how [the] Surveillance Technology has been used, including whether it captured images, sound, or other information regarding members of the public who are not suspected of engaging in unlawful conduct.**

This technology will be used by BHA Police. Four units of the technology have been acquired from Motorola. The acquired cameras will be deployed as part of Police Officer equipment. The technology will be deployed primarily in BHA communities, though the officers may interact with other communities across the City.

The technology is not yet deployed. BHA began acquiring technology between 2021 and 2022. The technology has not been deployed yet, so it has not captured any data regarding members of the public who are not suspected of engaging in unlawful conduct.

2. **Data Sharing: Whether and how often data acquired through the use of the Surveillance Technology was shared with local, state, and federal [agencies], the name of any recipient entity, the type(s) of data disclosed, any legal standard(s) under which the information was disclosed, and the justification for the disclosure.**

N/A

3. **Complaints: A summary of community complaints or concerns about the Surveillance Technology, if any.**

No.

4. **Audits: The results of any internal audits, any information about violations of the Surveillance Use Policy, and any actions taken in response other than to the extent that such inclusion would violate the privacy rights of an employee of the City.**

The Department has not conducted any formal audits.

5. **Effectiveness: A detailed accounting of whether the Surveillance Technology has been effective at achieving its identified purpose.**

The identified purpose of body worn cameras is to provide transparency and accountability. The technology has not been deployed yet.

6. **Public Records Requests: The number of public records requests received by the City seeking documents *concerning* Surveillance Technologies approved during the previous year.**

None have been received.

7. **Cost: An estimate of the total annual costs for the Surveillance Technology, including personnel and other ongoing costs, and what source(s) of funding will fund the technology in the coming year, if known.**

There were no costs associated with this technology in 2023.

8. **Impact on Communities: Whether the civil rights and liberties of any communities or groups, including communities of color or other marginalized communities in the City, are disproportionately impacted by the deployment of the Surveillance Technology.**

The technology has not been deployed, and there have been no concerns within the BHA or externally to BHA about the civil rights and liberties impact of this technology.

9. **Agreements: A disclosure of any new agreements made in the past 12 months with non-City entities that may include acquiring, sharing, or otherwise using [the] Surveillance Technology or the Surveillance Data it provides.**

No new agreements have been made in the past 12 months.

Department: Boston Housing Authority
Surveillance Technology: Decibel Meters

1. **Description: A description of how [the] Surveillance Technology has been used, including whether it captured images, sound, or other information regarding members of the public who are not suspected of engaging in unlawful conduct.**

The technology will be used by BHA police. We have acquired 0 units of the technology, and the technology has not been used by any positions. BHA's intent is to maximize effective use of personnel and improve response to quality of life issues. The department started acquiring the technology between 2021-2022. The technology has not been used to capture data regarding members of the public who are not suspected of engaging in unlawful conduct.

2. **Data Sharing: Whether and how often data acquired through the use of the Surveillance Technology was shared with local, state, and federal [agencies], the name of any recipient entity, the type(s) of data disclosed, any legal standard(s) under which the information was disclosed, and the justification for the disclosure.**

N/A

3. **Complaints: A summary of community complaints or concerns about the Surveillance Technology, if any.**

There have been no community complaints or concerns about the Surveillance Technology.

4. **Audits: The results of any internal audits, any information about violations of the Surveillance Use Policy, and any actions taken in response other than to the extent that such inclusion would violate the privacy rights of an employee of the City.**

No audits have been conducted regarding use of the technology.

5. **Effectiveness: A detailed accounting of whether the Surveillance Technology has been effective at achieving its identified purpose.**

The identified purpose of BHA decibel meters is to maximize effective use of personnel and address quality of life concerns. On a scale from 1 to 5, BHA would rate the effectiveness at level 2 at this time. The technology has not been deployed yet.

6. **Public Records Requests: The number of public records requests received by the City seeking documents *concerning* Surveillance Technologies approved during the previous year.**

BHA has received no public records requests concerning this surveillance technology.

7. **Cost: An estimate of the total annual costs for the Surveillance Technology, including personnel and other ongoing costs, and what source(s) of funding will fund the technology in the coming year, if known.**

There were no costs associated with this technology in 2023.

8. **Impact on Communities: Whether the civil rights and liberties of any communities or groups, including communities of color or other marginalized communities in the City, are disproportionately impacted by the deployment of the Surveillance Technology.**

Not applicable, since the technology has not been deployed yet.

9. **Agreements: A disclosure of any new agreements made in the past 12 months with non-City entities that may include acquiring, sharing, or otherwise using [the] Surveillance Technology or the Surveillance Data it provides.**

No new agreements have been made in the past 12-months with any non-City entities.

Department: Boston Municipal Protective Services
Surveillance Technology: Security Camera Network and Video Management System

1. **Description: A description of how [the] Surveillance Technology has been used, including whether it captured images, sound, or other information regarding members of the public who are not suspected of engaging in unlawful conduct.**

Cameras are installed on City property for security purposes, including closed-circuit television cameras to monitor entryways and outdoor areas of City-owned or controlled buildings and property for the purpose of controlling access, maintaining the safety of City employees and visitors to City buildings, and protecting City property. Some security cameras including closed-circuit television cameras monitor cashiers' windows and other cash-handling operations and to maintain the safety of City employees and visitors to such areas. Cameras installed to protect the physical integrity of City infrastructure. The Department has replaced 29 existing cameras and added 81 new cameras to the network this past year as a result of the Department assuming property management responsibilities for the Boston Centers for Youth and Families (BCYF) facilities. Cameras have been in use since prior to 2021.

The cameras are monitored by security officers and when alarms are triggered by our alarm monitoring operators. On limited occasions, Department managers view camera footage, such as when requested by the Office of Human Resources or Office of Labor Relations for employee investigations. The cameras are installed exclusively in City owned buildings in all neighborhoods, but not in all City-owned buildings. This specific information can be made available if needed. Some security cameras are actively monitored primarily during daytime working hours. Other cameras may be monitored after working hours in response to alarms triggered.

The cameras capture video only, not sound. The cameras may capture members of the public who pass through or occupy the field of view, including those who are not suspected of engaging in unlawful conduct. Most of our cameras have a limited field of view and the video quality decreases during bad weather or at night.

2. **Data Sharing: Whether and how often data acquired through the use of the Surveillance Technology was shared with local, state, and federal [agencies], the name of any recipient entity, the type(s) of data disclosed, any legal standard(s) under which the information was disclosed, and the justification for the disclosure.**

Data has been shared with a local entity–specifically, the data has been shared through the Law Department Public Records team. The Department shares data with the Law Department Public Records team. We upload camera video to the GovQA website if the video is responsive to a public records request and not otherwise exempt.

3. **Complaints: A summary of community complaints or concerns about the Surveillance Technology, if any.**

We have not received any community complaints on this technology. On one occasion, a Boston Planning and Development Agency employee asked for a copy of a video to support his complaint that he was unfairly treated by the Municipal Protective Services (MPS) Department. Our Commissioner reviewed the video and discussed the incident with the employee and it was resolved satisfactorily.

4. **Audits: The results of any internal audits, any information about violations of the Surveillance Use Policy, and any actions taken in response other than to the extent that such inclusion would violate the privacy rights of an employee of the City.**

We have not conducted an internal audit regarding the technology. However, we do communicate with representatives of the Department of Innovation and Technology, and other Departments on the use and policy of security cameras. We work together to implement best practices in use of the cameras and in procuring the best quality equipment and licensing and software upgrades.

We have not received any incidents of a violation of the Surveillance Use Policy. Access to export camera video is restricted to only two Department employees who work closely with the senior leadership.

5. **Effectiveness: A detailed accounting of whether the Surveillance Technology has been effective at achieving its identified purpose.**

The Department uses security cameras to monitor buildings and grounds to control access, maintain the safety of City employees and visitors to City buildings, and to protect City property. The technology has been extremely effective in achieving its identified purpose. The security cameras represent best practices in the field of property management. The cameras act as a crime deterrent and are very effective at helping the Department monitor buildings and grounds to control access, protect property, and maintain the safety of employees and visitors.

6. **Public Records Requests: The number of public records requests received by the City seeking documents *concerning* Surveillance Technologies approved during the previous year.**

The Department received eleven (11) public record requests for camera video in 2023.

7. **Cost: An estimate of the total annual costs for the Surveillance Technology, including personnel and other ongoing costs, and what source(s) of funding will fund the technology in the coming year, if known.**

The Department spent approximately $6,522 on camera equipment and $40,024 on a maintenance contract with our integrator, Siemens Industry, Inc.

8. **Impact on Communities: Whether the civil rights and liberties of any communities or groups, including communities of color or other marginalized communities in the City, are disproportionately impacted by the deployment of the Surveillance Technology.**

There are no communities that are disproportionately impacted by the deployment of the Surveillance Technology. Some security cameras are actively monitored primarily during daytime working hours. Other cameras may be monitored after working hours in response to alarms triggered.

9. **Agreements: A disclosure of any new agreements made in the past 12 months with non-City entities that may include acquiring, sharing, or otherwise using [the] Surveillance Technology or the Surveillance Data it provides.**

N/A

Department: Boston Municipal Protective Services
Surveillance Technology: Shooter Detection Technology, Guardian System

1. **Description: A description of how [the] Surveillance Technology has been used, including whether it captured images, sound, or other information regarding members of the public who are not suspected of engaging in unlawful conduct.**

The Shooter Detection Technology, Guardian System, is intended to identify a potential active shooter with sensors in 10 locations and 29 cameras in entrance lobbies, the loading dock, Mayor's Office, City Council Chamber, and near large public meeting rooms in City Hall. The sensors (which capture sound and light) are always on and trigger the system when they detect the sound of a gunshot or muzzle flash.

The shooter detection system is only deployed inside City Hall. When triggered, the system activates surveillance cameras in the specific location of the discharge and transmits a still photo and location information by email and text alert to a predefined list of recipients. The capability includes a building-wide broadcast over the public address system. The technology was installed with OEM grant funding and installation completed in February 2018. To date, no active shooter incidents have occurred. The Department is now working with our partners to reinstitute full operational capability.

The technology has not captured any information regarding members of the public who are not suspected of engaging in unlawful conduct. If the system is fully operational, and in the remote likelihood of activation, it could potentially capture a still photo image of members of the public in the immediate vicinity of an active shooter if a gunshot or muzzle flash is detected. The system is designed to work and collect information only in the event of an actual gunshot. The Department has other security protocols in place to minimize the risk of an active shooter scenario, including security screening with x-ray machines and metal detectors.

No additional units have been acquired in the past year, and the technology has not been fully implemented to date and the portions of it that have been implemented have not been activated by an active shooter (see next question). If the technology was activated, it would notify Municipal Protective Services (MPS) officers and designated Administration Officials of a potential active shooter incident. In the future, the technology may be used to broadcast a recording to employees throughout the building using an existing public address system.

The sensor technology is always on, but the actual surveillance system has not been triggered to date. The technology was acquired before 2021.

2. **Data Sharing: Whether and how often data acquired through the use of the Surveillance Technology was shared with local, state, and federal [agencies], the name of any recipient entity, the type(s) of data disclosed, any legal standard(s) under which the information was disclosed, and the justification for the disclosure.**

The data has only been shared with limited staff in DoIT and OEM.

3. **Complaints: A summary of community complaints or concerns about the Surveillance Technology, if any.**

We have received no community complaints or concerns about the Surveillance Technology.

4. **Audits: The results of any internal audits, any information about violations of the Surveillance Use Policy, and any actions taken in response other than to the extent that such inclusion would violate the privacy rights of an employee of the City.**

The Department has not conducted a formal audit, but is working with the Department of Innovation and Technology (DoIT) and Office of Emergency Services (OEM) to improve the capability of the technology. There are no documented violations of the Surveillance Use Policy relevant to this technology.

5. **Effectiveness: A detailed accounting of whether the Surveillance Technology has been effective at achieving its identified purpose.**

The purpose of the Shooter Detection Systems Company Guardian System is to identify a potential active shooter with acoustical sensors in 10 locations and 29 cameras in entrance lobbies, the loading dock, Mayor's Office, City Council Chamber, and near large public meeting rooms in City Hall by detecting a firearm discharge and activating surveillance cameras in the specific location of the discharge. The system would immediately notify select personnel.

On a scale from 1 to 5, we would rate the effectiveness at level 2 at this time. The technology is active but not fully implemented at this time, meaning not all intended public buildings and spaces are fully covered by the technology. In the future, we anticipate the effectiveness rating will increase to 5, once fully operational.

6. **Public Records Requests: The number of public records requests received by the City seeking documents *concerning* Surveillance Technologies approved during the previous year.**

There have been no public records requests received by the City concerning this Surveillance Technology.

7. **Cost: An estimate of the total annual costs for the Surveillance Technology, including personnel and other ongoing costs, and what source(s) of funding will fund the technology in the coming year, if known.**

The total annual costs for this technology are minimal. We procured one piece of equipment for $4,269 to simplify access to video still shots in the event of the sound of gunfire or a muzzle flash by replacing a forward-looking infrared server with a plug-in to our existing camera VMS. We anticipate operating costs in the coming year will be low and we will use operating funds.

8. **Impact on Communities: Whether the civil rights and liberties of any communities or groups, including communities of color or other marginalized communities in the City, are disproportionately impacted by the deployment of the Surveillance Technology.**

The technology has not been used to date in our facility.

9. **Agreements: A disclosure of any new agreements made in the past 12 months with non-City entities that may include acquiring, sharing, or otherwise using [the] Surveillance Technology or the Surveillance Data it provides.**

N/A

Department: Boston Public Schools
Surveillance Technology: Video Management System

1. **Description: A description of how [the] Surveillance Technology has been used, including whether it captured images, sound, or other information regarding members of the public who are not suspected of engaging in unlawful conduct.**

The cameras are used for security purposes. The technology is deployed in various Boston Public Schools buildings. The technology is in continual use, and doesn't have a specific use case. Cameras were acquired before 2021. BPS is unsure whether the technology has been used to capture data regarding members of the public who are not suspected of engaging in unlawful conduct.

2. **Data Sharing: Whether and how often data acquired through the use of the Surveillance Technology was shared with local, state, and federal [agencies], the name of any recipient entity, the type(s) of data disclosed, any legal standard(s) under which the information was disclosed, and the justification for the disclosure.**

Video captured by surveillance cameras is shared with local and state entities pursuant to federal restrictions governing student records. In the case of an imminent emergency, videos are viewed by law enforcement. If the BPS receives a subpoena, warrant, or court order, the video (footage) is provided to the District Attorney's Office and in cases involving child abuse or neglect, video footage may be provided to DCF.

FERPA protects video images of students and subpoenas are required to obtain copies. Parents of students depicted may view footage. Video images of non students may be disclosed pursuant to public records requests if student and staff safety is not compromised.

3. **Complaints: A summary of community complaints or concerns about the Surveillance Technology, if any.**

BPS has received no concerns or complaints about the Surveillance Technology.

4. **Audits: The results of any internal audits, any information about violations of the Surveillance Use Policy, and any actions taken in response other than to the extent that such inclusion would violate the privacy rights of an employee of the City.**

None.

5. **Effectiveness: A detailed accounting of whether the Surveillance Technology has been effective at achieving its identified purpose.**

The technology's identified purpose is the security for students and staff attending school. Security cameras are known for deterring criminals from threatening the safety of students and staff. On a 5-point scale, BPS would give the cameras a "4" rating for effectiveness.

6. **Public Records Requests: The number of public records requests received by the City seeking documents *concerning* Surveillance Technologies approved during the previous year.**

BPS has received 10-15 public records requests concerning Surveillance Technologies.

7. **Cost: An estimate of the total annual costs for the Surveillance Technology, including personnel and other ongoing costs, and what source(s) of funding will fund the technology in the coming year, if known.**

In 2023, BPS spent $1,809,412 on security cameras and cabling installation.

8. **Impact on Communities: Whether the civil rights and liberties of any communities or groups, including communities of color or other marginalized communities in the City, are disproportionately impacted by the deployment of the Surveillance Technology.**

N/A

9. **Agreements: A disclosure of any new agreements made in the past 12 months with non-City entities that may include acquiring, sharing, or otherwise using [the] Surveillance Technology or the Surveillance Data it provides.**

No new agreements have been made with non-City entities.

Department: Office of Emergency Management
Surveillance Technology: Critical Infrastructure Monitoring System

1. **Description: A description of how [the] Surveillance Technology has been used, including whether it captured images, sound, or other information regarding members of the public who are not suspected of engaging in unlawful conduct.**

OEM supports the maintenance of this system and administrative procurement. Cameras are procured from Lan-Tel Communications, Inc. OEM does not determine where cameras are placed. Please contact the Boston Police Department for additional information.

OEM utilizes live video footage during activations of the Emergency Operations Center (EOC) and to maintain situational awareness and a posture of readiness during developing incidents. This technology is deployed across the City. Please consult the Boston Police Department for further information.

These cameras have been used for events such as the Boston Marathon, 4th of July Celebration, and other large events. Cameras were acquired before 2021, and have been used to capture images, sounds, and other information regarding members of the public who are not suspected of engaging in unlawful conduct.

2. **Data Sharing: Whether and how often data acquired through the use of the Surveillance Technology was shared with local, state, and federal [agencies], the name of any recipient entity, the type(s) of data disclosed, any legal standard(s) under which the information was disclosed, and the justification for the disclosure.**

Local, State, and private sector partners present during activations are able to see live video presented for situational awareness. Please consult the Boston Police Department for additional information.

3. **Complaints: A summary of community complaints or concerns about the Surveillance Technology, if any.**

OEM has not received any complaints or concerns regarding use of the technology.

4. **Audits: The results of any internal audits, any information about violations of the Surveillance Use Policy, and any actions taken in response other than to the extent that such inclusion would violate the privacy rights of an employee of the City.**

No internal audits have been conducted. There have been no incidents where the Surveillance Use Policy was violated.

5. **Effectiveness: A detailed accounting of whether the Surveillance Technology has been effective at achieving its identified purpose.**

The identified purpose of this technology is to utilize live video footage during activations of the Emergency Operations Center (EOC) and to maintain situational awareness and a posture of readiness

during developing incidents. OEM would rate the effectiveness of the technology at a 5 on a 5-point scale. The system currently provides sufficient situational awareness during developing incidents.

6. **Public Records Requests: The number of public records requests received by the City seeking documents *concerning* Surveillance Technologies approved during the previous year.**

OEM has received no public records requests by the City seeking documents concerning this Surveillance Technology.

7. **Cost: An estimate of the total annual costs for the Surveillance Technology, including personnel and other ongoing costs, and what source(s) of funding will fund the technology in the coming year, if known.**

Federally-granted Urban Area Security Initiative grant funding, managed by the City on behalf of the Metro Boston Homeland Security Region (MBHSR), funds the annual maintenance of the CIMS network at about $600,000 per year.

There were no costs associated with this technology within OEM in 2023.

8. **Impact on Communities: Whether the civil rights and liberties of any communities or groups, including communities of color or other marginalized communities in the City, are disproportionately impacted by the deployment of the Surveillance Technology.**

We are not aware of any civil rights and liberties of communities or groups disproportionately affected by the deployment of the Surveillance Technology.

9. **Agreements: A disclosure of any new agreements made in the past 12 months with non-City entities that may include acquiring, sharing, or otherwise using [the] Surveillance Technology or the Surveillance Data it provides.**

There are no new agreements made in the past 12 months with non-City entities concerning use of this technology.

Department: Parks Department
Surveillance Technology: Asset Management Cameras

1. **Description: A description of how [the] Surveillance Technology has been used, including whether it captured images, sound, or other information regarding members of the public who are not suspected of engaging in unlawful conduct.**

The cameras are only used for asset management purposes by the Boston Parks Department. Boston Parks has installed these cameras, but does not manage them. If footage was needed for asset management purposes (i.e. after City property was damaged or defaced), the Parks department would request footage from Boston Police who monitor our cameras. The Park Department has not used the footage from these cameras this year, but Boston Police Department (who manage the system), may have used it. All footage is captured, stored, and managed by the Boston Police Department, not the Boston Parks Department.

The Parks Department has acquired nine units at three sites in the past year. The three sites where these cameras were deployed this year are in Roxbury and Dorchester.

It is very possible, if not likely, that these cameras have captured information regarding members of the public who are not suspected of engaging in unlawful conduct, but these cameras are clearly visible near City property, typically on existing light poles.

2. **Data Sharing: Whether and how often data acquired through the use of the Surveillance Technology was shared with local, state, and federal [agencies], the name of any recipient entity, the type(s) of data disclosed, any legal standard(s) under which the information was disclosed, and the justification for the disclosure.**

N/A

3. **Complaints: A summary of community complaints or concerns about the Surveillance Technology, if any.**

We have not received any community complaints or concerns about the Surveillance Technology.

4. **Audits: The results of any internal audits, any information about violations of the Surveillance Use Policy, and any actions taken in response other than to the extent that such inclusion would violate the privacy rights of an employee of the City.**

The Parks Department has not conducted any internal audits of the Surveillance Technology. There have not been any violations of the Surveillance Use Policy.

5. **Effectiveness: A detailed accounting of whether the Surveillance Technology has been effective at achieving its identified purpose.**

The purpose of the Surveillance Technology is asset management, at the request of the community during a community process. These cameras were installed at the request of the community during a community process for asset management purposes. These requests typically come directly in response to destruction of City property, vandalism, graffiti, etc. Installing these cameras directly responds to stated community needs. We would say the cameras have been extremely effective in fulfilling their identified purpose.

6. **Public Records Requests: The number of public records requests received by the City seeking documents *concerning* Surveillance Technologies approved during the previous year.**

The Parks Department has not received any public records request for camera footage in Parks, nor would the Parks Department be notified if BPD received a public records request for footage captured from these cameras.

7. **Cost: An estimate of the total annual costs for the Surveillance Technology, including personnel and other ongoing costs, and what source(s) of funding will fund the technology in the coming year, if known.**

The Boston Parks Department does not assume an annual cost other than installation, which is typically lumped into an overall capital construction cost. In this context, the addition of cameras is a relatively cheap amount.

8. **Impact on Communities: Whether the civil rights and liberties of any communities or groups, including communities of color or other marginalized communities in the City, are disproportionately impacted by the deployment of the Surveillance Technology.**

No, to the knowledge of the Parks Department there are no communities that are disproportionately impacted by the deployment of the Surveillance Technology.

9. **Agreements: A disclosure of any new agreements made in the past 12 months with non-City entities that may include acquiring, sharing, or otherwise using [the] Surveillance Technology or the Surveillance Data it provides.**

N/A

Department: Boston Police Department
Surveillance Technology: Automated License Plate Recognition System

1. **Description: A description of how [the] Surveillance Technology has been used, including whether it captured images, sound, or other information regarding members of the public who are not suspected of engaging in unlawful conduct.**

The Boston Police Department Automated License Plate Recognition (ALPR) System is a computer-based system that utilizes special fixed cameras to take digital images of a license plate and/or motor vehicle. Boston Police Department Special Order 16-031 (Automated License Plate Recognition System) governs the use of the Department's ALPR System.

As of December 31, 2023, the Department operates fewer than ten License Plate Readers.

The ALPR System captures an infrared image of a license plate and converts it to a text file using Optical Character Recognition ("OCR") technology. Data available in the ALPR System also includes the time and geographic coordinates associated with the digital image that was captured. The ALPR cameras do not record video, do not capture sound, and cannot be viewed in real-time.

The text file is compared to Vehicle of Interest (VOI) lists generated by law enforcement agencies, including the National Crime Information Center, Massachusetts Department of Criminal Justice Information Services, and the Boston Police Department, to search for a "hit" or potential match. The VOI lists include vehicles that have been stolen, vehicles associated with Amber Alerts, vehicles wanted in connection with specific crimes, and vehicles associated with, or that may assist with the identification of, suspects involved in criminal activity.

The ALPR System is used for legitimate law enforcement purposes and the enhancement of public safety, such a:s, providing information to officers that will assist in on-going criminal investigations, crime prevention, the apprehension of wanted persons, ensuring the safety of vulnerable individuals through the recovery of missing and endangered persons, and identifying and removing stolen motor vehicles.

2. **Data Sharing: Whether and how often data acquired through the use of the Surveillance Technology was shared with local, state, and federal [agencies], the name of any recipient entity, the type(s) of data disclosed, any legal standard(s) under which the information was disclosed, and the justification for the disclosure.**

Please see attached spreadsheet of requests to provide data received in 2023.

The Operations Division Duty Supervisor may approve a mutual aid request from other law enforcement agencies for use of the ALPR System for purposes consistent with BPD Special Order 16-031, as may be appropriate under the circumstances and as resources permit. Operations Division Duty Supervisors are encouraged to provide mutual aid to other communities when they become aware of a serious incident that they reasonably believe the ALPR System may be useful for. Examples of serious incidents include homicides, shootings, kidnappings, sexual assaults, AMBER alerts, or other serious or violent felonies as to which suspect vehicle information is available.

All requests made from other law enforcement agencies are handled in accordance with all relevant federal and state laws, BPD rules and regulations, including, but not limited to Special Order 21-46 (Outside Agency Notification), and local ordinances including, but not limited to, Chapter 11-1.9 of the City of Boston Municipal Code (Boston Trust Act).

Criminal defendants receive data which is relevant and/or exculpatory to their case through the District Attorney's Office, Attorney General's Office, or United States Attorney's Office pursuant to the rules of discovery, including, but not limited to, Fed. R. Crim. P. 16 and Mass. R. Crim. P. 14, and in accordance with federal and state case law. Additionally, criminal defendants may seek a subpoena or other court order to request the production of specific data pursuant to the rules of criminal procedure, including, but not limited to, Fed. R. Crim. P. 17 and Mass. R. Crim. P. 17.

3. **Complaints: A summary of community complaints or concerns about the Surveillance Technology, if any.**

In an attempt to thoroughly respond to this question, queries were made to the Department's Bureau Chiefs, which includes the Bureau of Field Services, the Bureau of Investigative Services, and the Bureau of Community Engagement, as well as to the individual District Community Service Offices. The Department has not located any specific complaint concerning this technology responsive to this request.

The Department is cognizant that there has been general discussion surrounding the use of technology in the City in various forums and that such discussion may have included complaints or concerns; however, these discussions often occur in forums outside of the Department and, as a result, the Department has been unable to locate any specific complaints relative to this technology.

4. **Audits: The results of any internal audits, any information about violations of the Surveillance Use Policy, and any actions taken in response other than to the extent that such inclusion would violate the privacy rights of an employee of the City.**

Audits: The Boston Police Department Audit and Review Unit is responsible for conducting, reviewing, and retaining audits of the ALPR System usage. Audits shall determine the Department's adherence to Special Order 16-031 as well as the maintenance and completeness of records. A copy of the periodic audit of the ALPR System conducted on October 18, 2023, is attached.

Discipline: Any employee who engages in an impermissible use of the ALPR System, data associated with the ALPR System, or VOI lists may be subject to disciplinary action up to and including termination. Compliance with all BPD Policies, Procedures, Rules, SOPs, and Special Orders is monitored by the Bureau of Professional Standards, Internal Affairs Division (IAD). *See* BPD Rule 102 (The Conduct and General Responsibilities of Department Personnel) and BPD Rule 109 (Discipline Procedure).

In 2023, there were no IAD complaints with an allegation of misuse of the ALPR System or data.

5. **Effectiveness: A detailed accounting of whether the Surveillance Technology has been effective at achieving its identified purpose.**

The ALPR System is used for legitimate law enforcement purposes and the enhancement of public safety, such as, providing information to officers that will assist in on-going criminal investigations, crime prevention, the apprehension of wanted persons, ensuring the safety of vulnerable individuals through the recovery of missing and endangered persons, and identifying and removing stolen motor vehicles.

Please see attachment regarding the effectiveness of the Department's surveillance technology.

6. **Public Records Requests: The number of public records requests received by the City seeking documents concerning Surveillance Technologies approved during the previous year.**

The Department received 1 request for information specifically regarding the ALPR System or data.

Public records requests often include a request for any and all information relating to the subject of the request. Due to the broad nature of those requests, the responsive documents could potentially include information relative to this technology. With that in mind, and in order to capture all responsive information to this request, the Department received 5,879 public records requests in 2023, including the specific request for information regarding the ALPR System or data. A spreadsheet of all the requests is attached.

7. **Cost: An estimate of the total annual costs for the Surveillance Technology, including personnel and other ongoing costs, and what source(s) of funding will fund the technology in the coming year, if known.**

In FY 2023, the Department did not have any expenditures for ALPRs.

Information regarding the Department's FY2023 and FY2024 costs and expenditures is publicly available at: https://www.boston.gov/departments/budget/fy23-operating-budget and https://www.boston.gov/departments/budget/fy24-operating-budget. Information regarding the Department's FY2023 and FY2024 grant funding is attached. The Department's purchases of technology are made through the City of Boston procurement process.

The Department does not have any dedicated personnel cost for this technology.

8. **Impact on Communities: Whether the civil rights and liberties of any communities or groups, including communities of color or other marginalized communities in the City, are disproportionately impacted by the deployment of the Surveillance Technology.**

The Boston Police Department strives to maintain the highest standards of honesty and integrity and is committed to building and strengthening trust with all members of the community. *See* BPD Rule 113 (Public Integrity Policy) and BPD Rule 113A (Bias-Free Policing Policy). All members of the Boston Police Department (sworn and civilian) are committed to providing services and enforcing laws in a professional, nondiscriminatory, fair, and equitable manner. This includes services involving the use of this technology. The Boston Police Department is committed to bias-free policing. *See* BPD Rule 113A (Bias-Free Policing Policy).

The Department is not aware of any finding, outcome, or determination of disparate impact involving this technology.

9. **Agreements: A disclosure of any new agreements made in the past 12 months with non-City entities that may include acquiring, sharing, or otherwise using [the] Surveillance Technology or the Surveillance Data it provides.**

In 2023, the Department did not enter into any new agreements with non-City entities to acquire, share, or utilize the technology to expand the Department's capabilities beyond those that have been previously reported.

Attachments:

a) ALPR Data Sharing Requested 2023
b) ALPR System Audit 2023

Department: Boston Police Department
Surveillance Technology: Cameras and Video Management Systems (VMS)

1. **Description: A description of how [the] Surveillance Technology has been used, including whether it captured images, sound, or other information regarding members of the public who are not suspected of engaging in unlawful conduct.**

The Boston Police Department is dedicated to ensuring public safety in our neighborhoods while balancing civil rights and privacy protections. Video management systems are a tremendous tool for the department in criminal investigations, at large scale events, to protect critical infrastructure, and for other official law enforcement purposes.

For example, the Department's cameras and video management systems may be used to:

- deter criminal activity and public disorder
- reduce fear of crime
- identify criminal activity and suspects
- identify and gather possible evidence for use in criminal and civil court actions
- document police actions
- safeguard citizen and police officer rights
- aid in Amber alerts or in the search for lost/missing children or elderly people
- assist emergency services personnel when responding to incidents
- assist with the monitoring of traffic conditions
- evacuation route status
- monitor transportation networks (airports, waterways, highways, tunnels, transit, intermodal), events and attractions, government facilities, severe weather events
- assist officials with the provision of municipal services in order to enhance overall municipal efficiency
- assist with the training of department personnel.

As of December 31, 2023, BPD's Bureau of Administration and Technology (BAT) maintains a network of approximately 1,300 cameras (the "BAT Camera System") throughout the City of Boston. These cameras are located on fixtures such as light poles, street signs, and buildings. Some of these cameras were purchased and are owned by private entities or neighborhood groups for the purpose of improving safety and security of their business, business district, or neighborhood. These cameras' location and placement was requested by these groups. These groups do not have access to the live stream or recorded video from these (or any) cameras on the BAT Camera System. During 2023, the Department used the FLIR Video Management System to view the cameras on the BAT Camera System. Beginning in early 2024, the Department began to utilize the Genetec Video Management System to view these cameras.

The Boston Police Department has direct access to approximately 400 additional cameras that are owned and maintained by the City of Boston (DoIT) and the Boston Transportation Department (BTD) (the "DoIT/BTD Camera System"). The Department uses the Genetec Video Management System to view the cameras on the DoIT/BTD Camera System.

The video cameras capture video only - live stream and recording ("VMS Video"). The BAT Camera System and the DoIT/BTD Camera System are active twenty-four (24) hours a day, seven (7) days a week ("24/7"). The Department does not monitor the live stream of the BAT Camera System or DoIT/BAT Camera System 24/7.

Cameras on both systems may have pan-tilt-zoom ("PTZ") or thermal capability. Thermal cameras are near water to show heat differential where visibility is reduced.

The cameras do not have facial recognition capabilities. The cameras do not have any audio capabilities.

2. **Data Sharing: Whether and how often data acquired through the use of the Surveillance Technology was shared with local, state, and federal [agencies], the name of any recipient entity, the type(s) of data disclosed, any legal standard(s) under which the information was disclosed, and the justification for the disclosure.**

Please see attached spreadsheet for requests the VEU received in 2023 to provide recorded video from the BAT and DoIT/BTD Camera Systems.

If the surveillance data is relevant to a criminal case or investigation, all discovery requests or subpoenas made by federal and state prosecutors are directed to the primary investigator assigned to the case. The primary investigator will put in a written request to the VEU seeking a copy of the relevant recordings. The VEU provides a DVD copy of the recording to the investigator who will then provide copies to the prosecutor.

Outside Jurisdictions: Any request for live feed access made by an outside jurisdiction is reviewed for approval through the BPD Bureau of Administration and Technology. If granted, the BPD Telecommunications system administrator will take the necessary steps to activate the connection. If approved, access is granted for a specific time period and only for cameras relevant to the request. This approval and access process will be documented and maintained by the Bureau of Administration and Technology.

Metro Boston Homeland Security Region (MBHSR) Jurisdictions: A jurisdiction within the MBHSR may request archived camera footage from another jurisdiction in the event of a criminal investigation or access to live camera footage in instances such as preplanned major events (i.e., Boston Marathon). In the event that access is granted to an outside jurisdiction, the record of access will be documented and stored to capture the incident number, name of requestor, as well as the location and time of the requested video evidence.

A requesting jurisdiction within the MBHSR will have the ability to view images/video produced by the Critical Infrastructure Monitoring System/VMS cameras only after the BPD has authorized and granted such access. The Police Commissioner or their designee shall have exclusive authority to authorize other jurisdictions within the MBHSR access to footage recorded by the CIMS/VMS cameras. Access will only include live viewing and/or review viewing (rewinding). It will not include the ability to download or record.

A MBHSR Jurisdiction may also request a copy of archival footage pursuant to the MBHSR CIMS policy.

All requests made from other law enforcement agencies are handled in accordance with all relevant federal and state laws, BPD rules and regulations, including, but not limited to Special Order 21-46 (Outside Agency Notification), and local ordinances including, but not limited to, Chapter 11-1.9 of the City of Boston Municipal Code (Boston Trust Act).

3. **Complaints: A summary of community complaints or concerns about the Surveillance Technology, if any.**

In an attempt to thoroughly respond to this question, queries were made to the Department's Bureau Chiefs, which includes the Bureau of Field Services, the Bureau of Investigative Services, and the Bureau of Community Engagement, as well as to the individual District Community Service Offices.

The Department received one complaint from a community member that questioned the placement of a camera in his neighborhood and whether it was directed towards his residence. The Department reviewed this complaint and determined that the camera in question was placed on a public way and not in contravention to any Department rule; the cameras in this area are fixed and not directed at a particular residence.

The Department is cognizant that there has been general discussion surrounding the use of technology in the City in various forums and that such discussion may have included complaints or concerns; however, these discussions often occur in forums outside of the Department and, as a result, the Department has been unable to locate any specific complaints relative to this technology.

On the other hand, the Department has received feedback from the residential and business community requesting additional equipment or expansion of existing technology, including specifically for additional cameras.

4. **Audits: The results of any internal audits, any information about violations of the Surveillance Use Policy, and any actions taken in response other than to the extent that such inclusion would violate the privacy rights of an employee of the City.**

Audits: The BAT and BTD/DoIT Camera Systems have audit capabilities. All activity is recorded each time an employee logs into the system. All user activity is logged and maintained by the Department.

The CIMS project is overseen and managed by the MBHSR Jurisdictional Point of Contact (JPOC) Committee. The Critical Infrastructure and Key Resources (CIKR) Subcommittee will support the JPOC Committee with recommendations based upon subject matter expertise.

In addition, the MBHSR will routinely conduct audits to study funding decisions and their impact in order to better improve the CIMS program and make fiscally sound decisions. To ensure transparency and communication with local governments, the Boston Office of Emergency Management will provide an annual report compiled from audits performed by individual jurisdictions. These reports will identify the number of CIMS cameras within a jurisdiction, the number of users on the network and their permission levels, the number of archived video requests that were approved for footage on CIMS cameras, as well as the number of instances where real-time camera access was granted by a jurisdiction to a requesting agency.

Discipline: Compliance with all BPD Policies, Procedures, Rules, SOPs, and Special Orders is monitored by the Bureau of Professional Standards, Internal Affairs Division. *See* BPD Rule 102 (The Conduct and General Responsibilities of Department Personnel) and BPD Rule 109 (Discipline Procedure).

In 2023, there was 1 IAD complaint with an allegation of misuse of the cameras or VMS; the internal investigation is ongoing.

5. Effectiveness: A detailed accounting of whether the Surveillance Technology has been effective at achieving its identified purpose.

Cameras are a tremendous tool for the department in criminal investigations, at large scale events, to protect critical infrastructure and for other official law enforcement purposes. For example:

- In January 2023, officers responded to a radio call for shots fired on Prentiss Street and located a victim suffering from two gunshot wounds. Detectives utilized the BAT Camera System / FLIR to view the suspects who wore masks before and after the shooting. Detectives then utilized residential and commercial video to track the covered-up suspects by their clothing to the area of a housing development. Detectives pulled additional video from Boston Housing Authority and viewed the suspects in the same clothing unmasked. Detectives identified the suspects with these images and the Gang Assessment Database. Thereafter, a search warrant was executed and four (4) firearms were recovered.
- In February 2023, a caller reported shots fired in the area of Walnut Ave. Responding officers were initially unable to locate any victims or ballistics. RTCC Analysts observed the incident on the BAT Camera System. They relayed suspect and victim description, direction of flight, and directed officers to where the ballistics may be located. Officers recovered 7 shell casings.
- In March 2023, officers responded to a call for two individuals stabbed near Blue Hill Ave. In the initial call, a woman reported she was stabbed in the neck. A second victim approached officers and reported he was also stabbed to the neck by the same suspect. RTCC Analysts immediately reviewed video footage from the BAT Camera System cameras in the area and observed one individual matching the suspect description. A full suspect description, the description of a second individual observed with the suspect, and direction of flight was relayed to units. Officers responded to the area and stopped the suspect and placed him under arrest.
- In March 2023, RTCC Analysts responded to a call for an Armed Robbery (firearm) at Boost Mobile on Bowdoin St. Using the broadcasted suspect description, RTCC Analysts used the BAT Camera System to locate the suspect, gave the suspect's direction of flight to units in the field, and tracked the suspect using cameras in the area.
- In May 2023, a victim was found suffering from multiple stab wounds in Downtown Crossing and another victim reported being pepper sprayed and physically assaulted. RTCC Analysts were able to view the entire altercation on the BAT Camera System. They relayed where the crime scene was and were able to send stills of the parties involved. Officers made arrests shortly thereafter.
- In September 2023, officers responded to a radio call for a missing person with complications regarding an individual who had left his nursing home/rehab approximately twelve hours earlier. A photo of the man was disseminated, and officers utilized the BAT Camera System to locate the missing individual within the Boston Common.
- In September 2023, detectives were able to use surveillance cameras to help identify and track the movements of a young woman who was considered at risk of exploitation.
- In October 2023, officers responded to a radio call in the area of Stuart Street and Tremont Street for the report of a missing 8-year-old boy. Officers gathered a description of the boy from

his mother. Officers utilized the BAT Camera System, saw the boy in the area of Park Street Station, and broadcast their observations. Moments later, officers located the boy in Kenmore Square.

- In December 2023, the Nativity scene located inside the Boston Common was vandalized with spray paint. A review of the BAT Camera System video in the area yielded images of four suspects. The photo images were disseminated through BRIC bulletins and additional investigative leads developed through the review of surveillance video.

Please see attachment regarding the effectiveness of the Department's surveillance technology for additional details.

6. **Public Records Requests: The number of public records requests received by the City seeking documents concerning Surveillance Technologies approved during the previous year.**

The Department received 1,062 public records requests specifically for video from BAT and BTD/DoIT cameras.

Public records requests often include a request for any and all information relating to the subject of the request. Due to the broad nature of those requests, the responsive documents could potentially include information relative to this technology. With that in mind, and in order to capture all responsive information to this request, the Department received 5,879 public records requests in 2023, including the 1,062 requests specifically regarding video from BAT and BTD/DoIT cameras. A spreadsheet of all the requests is attached.

7. **Cost: An estimate of the total annual costs for the Surveillance Technology, including personnel and other ongoing costs, and what source(s) of funding will fund the technology in the coming year, if known.**

In FY 2023, the Department spent $341,477.53.

Information regarding the Department's FY2023 and FY2024 costs and expenditures is publicly available at: https://www.boston.gov/departments/budget/fy23-operating-budget and https://www.boston.gov/departments/budget/fy24-operating-budget. Information regarding the Department's FY2023 and FY2024 grant funding is attached. The Department's purchases of technology are made through the City of Boston procurement process.

The Department does not have any dedicated personnel cost for this technology.

8. **Impact on Communities: Whether the civil rights and liberties of any communities or groups, including communities of color or other marginalized communities in the City, are disproportionately impacted by the deployment of the Surveillance Technology.**

The Boston Police Department strives to maintain the highest standards of honesty and integrity and is committed to building and strengthening trust with all members of the community. *See* BPD Rule 113 (Public Integrity Policy) and BPD Rule 113A (Bias-Free Policing Policy). All members of the Boston Police Department (sworn and civilian) are committed to providing services and enforcing laws in a professional, nondiscriminatory, fair, and equitable manner. This includes services involving the use of

this technology. The Boston Police Department is committed to bias-free policing. *See* BPD Rule 113A (Bias-Free Policing Policy).

The Department is not aware of any finding, outcome, or determination of disparate impact involving this technology.

9. **Agreements: A disclosure of any new agreements made in the past 12 months with non-City entities that may include acquiring, sharing, or otherwise using [the] Surveillance Technology or the Surveillance Data it provides.**

The Boston Police Department, Brookline Police Department, and Boston Athletic Association entered into a short-term agreement to share live-stream video camera footage during the 127th Boston Marathon. A copy of the agreement is attached.

In 2023, the Department did not enter into any new agreements with non-City entities to acquire, share, or utilize the technology to expand the Department's capabilities beyond those that have been previously reported.

Attachments:

(a) Video Evidence Unit (VEU) Requests for Recorded Video 2023
(b) Boston Marathon Camera Sharing Agreement

Department: Boston Police Department
Surveillance Technology: Audio and Video Devices (Recording)

1. **Description: A description of how [the] Surveillance Technology has been used, including whether it captured images, sound, or other information regarding members of the public who are not suspected of engaging in unlawful conduct.**

All units of the Bureau of Investigative Services (BIS), the Bureau of Intelligence and Analysis (BIA), Boston Regional Intelligence Center (BRIC), all units of the Bureau of Field Services (BFS), and the Technology Services Division (TSD), Telecommunications Group use audio, video, and audio/video recording devices for legitimate law enforcement purposes and in furtherance of the Department's investigatory, public safety, and community caretaking responsibilities.

The audio, video and audio/video recording devices include, but are not limited to, the following:
- Hand-held audio recording devices (audio only)
- 911 call recording equipment (audio only)
- Cameras recording video at BPD District police stations (in public areas and holding areas) (video only)
- Department issued iPhones (audio and video)
- Audio/video equipment and systems at district stations used for recording witness and suspect interviews (audio and video)

2. **Data Sharing: Whether and how often data acquired through the use of the Surveillance Technology was shared with local, state, and federal [agencies], the name of any recipient entity, the type(s) of data disclosed, any legal standard(s) under which the information was disclosed, and the justification for the disclosure.**

Please see attached spreadsheet for requests the VEU received in 2023 to provide video from cameras at district police stations.

Audio and video data is shared with other law enforcement agencies for legitimate law enforcement purposes only. All requests made from other law enforcement agencies are handled in accordance with all relevant federal and state laws, BPD rules and regulations, including, but not limited to Special Order 21-46 (Outside Agency Notification), and local ordinances including, but not limited to, Chapter 11-1.9 of the City of Boston Municipal Code (Boston Trust Act).

Criminal defendants receive data which is relevant and/or exculpatory to their case through the District Attorney's Office, Attorney General's Office, or United States Attorney's Office pursuant to the rules of discovery, including, but not limited to, Fed. R. Crim. P. 16 and Mass. R. Crim. P. 14, and in accordance with federal and state case law. Additionally, criminal defendants may seek a subpoena or other court order to request the production of specific data pursuant to the rules of criminal procedure, including, but not limited to, Fed. R. Crim. P. 17 and Mass. R. Crim. P. 17.

3. **Complaints**: A summary of community complaints or concerns about the Surveillance Technology, if any.

In an attempt to thoroughly respond to this question, queries were made to the Department's Bureau Chiefs, which includes the Bureau of Field Services, the Bureau of Investigative Services, and the Bureau of Community Engagement, as well as to the individual District Community Service Offices. The Department has not located any specific complaint concerning this technology responsive to this request.

The Department is cognizant that there has been general discussion surrounding the use of technology in the City in various forums and that such discussion may have included complaints or concerns; however, these discussions often occur in forums outside of the Department and, as a result, the Department has been unable to locate any specific complaints relative to this technology.

4. **Audits: The results of any internal audits, any information about violations of the Surveillance Use Policy, and any actions taken in response other than to the extent that such inclusion would violate the privacy rights of an employee of the City.**

Audits: To the extent the technology supports user sign on, the Department utilizes a login with unique identification. All activity is recorded each time an employee logs into the system. All user activity is logged and maintained by the Department, establishing a corresponding audit trail.

Discipline: Compliance with all BPD Policies, Procedures, Rules, SOPs, and Special Orders is monitored by the Bureau of Professional Standards, Internal Affairs Division (IAD). *See* BPD Rule 102 (The Conduct and General Responsibilities of Department Personnel) and BPD Rule 109 (Discipline Procedure).

In 2023, there was 1 IAD complaint with an allegation of misuse of the audio and video (recording) devices; the allegation is under investigation.

5. **Effectiveness: A detailed accounting of whether the Surveillance Technology has been effective at achieving its identified purpose.**

Audio, video, and audio/video recording devices for legitimate law enforcement purposes and in furtherance of the Department's investigatory, public safety, and community caretaking responsibilities.

Please see attachment regarding the effectiveness of the Department's surveillance technology.

6. **Public Records Requests: The number of public records requests received by the City seeking documents concerning Surveillance Technologies approved during the previous year.**

The Department received public records requests for 911 calls, text messages and call logs from iPhones, audio and video recorded witness statements, and video recorded from cameras at District police stations. Public records requests often include a request for any and all information relating to the subject of the request. Due to the broad nature of those requests, the responsive documents could potentially include information relative to this technology. With that in mind, and in order to capture all responsive information to this request, the Department received 5,879 public records requests in 2023. A spreadsheet of all the requests is attached.

7. **Cost: An estimate of the total annual costs for the Surveillance Technology, including personnel and other ongoing costs, and what source(s) of funding will fund the technology in the coming year, if known.**

Information regarding the Department's FY2023 and FY2024 costs and expenditures is publicly available at: https://www.boston.gov/departments/budget/fy23-operating-budget and https://www.boston.gov/departments/budget/fy24-operating-budget. Information regarding the Department's FY2023 and FY2024 grant funding is attached. The Department's purchases of surveillance technology are made through the City of Boston procurement process.

The Department does not have any dedicated personnel cost for this technology.

8. **Impact on Communities: Whether the civil rights and liberties of any communities or groups, including communities of color or other marginalized communities in the City, are disproportionately impacted by the deployment of the Surveillance Technology.**

The Boston Police Department strives to maintain the highest standards of honesty and integrity and is committed to building and strengthening trust with all members of the community. *See* BPD Rule 113 (Public Integrity Policy) and BPD Rule 113A (Bias-Free Policing Policy). All members of the Boston Police Department (sworn and civilian) are committed to providing services and enforcing laws in a professional, nondiscriminatory, fair, and equitable manner. This includes services involving the use of this technology. The Boston Police Department is committed to bias-free policing. *See* BPD Rule 113A (Bias-Free Policing Policy).

The Department is not aware of any finding, outcome, or determination of disparate impact involving this technology.

9. **Agreements: A disclosure of any new agreements made in the past 12 months with non-City entities that may include acquiring, sharing, or otherwise using [the] Surveillance Technology or the Surveillance Data it provides.**

In 2023, the Department did not enter into any new agreements with non-City entities to acquire, share, or utilize the technology to expand the Department's capabilities beyond those that have been previously reported.

Attachments:

(a) Video Evidence Unit (VEU) Requests for District Police Station Recorded Video 2023

Department: Boston Police Department
Surveillance Technology: Audio and Video Devices (Non-Recording)

1. **Description: A description of how [the] Surveillance Technology has been used, including whether it captured images, sound, or other information regarding members of the public who are not suspected of engaging in unlawful conduct.**

The Boston Police Department Bureau of Field Services (BFS), SWAT, Special Operations Unit, and Youth Violence Strike Force (YVSF) use video and audio/video non-recording devices for legitimate law enforcement purposes and in furtherance of the Department's investigatory, public safety, and community caretaking responsibilities.

The following non-recording devices transmit real-time audio and/or video:
- "Throw Phone" with audio and video capabilities used by negotiators to communicate with barricaded individual(s)
- Fiber optic and pole cameras used for officer and community safety in potentially dangerous situations
- Cameras mounted on Boston Police Department vehicles

2. **Data Sharing: Whether and how often data acquired through the use of the Surveillance Technology was shared with local, state, and federal [agencies], the name of any recipient entity, the type(s) of data disclosed, any legal standard(s) under which the information was disclosed, and the justification for the disclosure.**

Access to the real-time audio and/or video is shared with other law enforcement agencies for legitimate law enforcement purposes only. All requests made from other law enforcement agencies are handled in accordance with all relevant federal and state laws, BPD rules and regulations, including, but not limited to Special Order 21-46 (Outside Agency Notification), and local ordinances including, but not limited to, Chapter 11-1.9 of the City of Boston Municipal Code (Boston Trust Act).

Criminal defendants receive data which is relevant and/or exculpatory to their case through the District Attorney's Office, Attorney General's Office, or United States Attorney's Office pursuant to the rules of discovery, including, but not limited to, Fed. R. Crim. P. 16 and Mass. R. Crim. P. 14, and in accordance with federal and state case law. Additionally, criminal defendants may seek a subpoena or other court order to request the production of specific data pursuant to the rules of criminal procedure, including, but not limited to, Fed. R. Crim. P. 17 and Mass. R. Crim. P. 17.

3. **Complaints: A summary of community complaints or concerns about the Surveillance Technology, if any.**

In an attempt to thoroughly respond to this question, queries were made to the Department's Bureau Chiefs, which includes the Bureau of Field Services, the Bureau of Investigative Services, and the Bureau of Community Engagement, as well as to the individual District Community Service Offices. The Department has not located any specific complaint concerning this technology responsive to this request.

4. **Audits: The results of any internal audits, any information about violations of the Surveillance Use Policy, and any actions taken in response other than to the extent that such inclusion would violate the privacy rights of an employee of the City.**

Audits: To the extent the technology supports user sign on, the Department utilizes a login with unique identification. All activity is recorded each time an employee logs into the system. All user activity is logged and maintained by the Department, establishing a corresponding audit trail.

Discipline: Compliance with all BPD Policies, Procedures, Rules, SOPs, and Special Orders is monitored by the Bureau of Professional Standards. *See* BPD Rule 102 (The Conduct and General Responsibilities of Department Personnel) and BPD Rule 109 (Discipline Procedure).

In 2023, there were no IAD complaints with an allegation of misuse of audio and video (non-recording) devices.

5. **Effectiveness: A detailed accounting of whether the Surveillance Technology has been effective at achieving its identified purpose.**

The Department uses video and audio/video non-recording devices for legitimate law enforcement purposes and in furtherance of the Department's investigatory, public safety, and community caretaking responsibilities.

Please see attachment regarding the effectiveness of the Department's surveillance technology.

6. **Public Records Requests: The number of public records requests received by the City seeking documents concerning Surveillance Technologies approved during the previous year.**

This technology is used in real-time and does not record.

Public records requests often include a request for any and all information relating to the subject of the request. Due to the broad nature of those requests, the responsive documents could potentially include information relative to this technology. With that in mind, and in order to capture all responsive information to this request, the Department received 5,879 public records requests in 2023. A spreadsheet of all the requests is attached.

7. **Cost: An estimate of the total annual costs for the Surveillance Technology, including personnel and other ongoing costs, and what source(s) of funding will fund the technology in the coming year, if known.**

Information regarding the Department's FY2023 and FY2024 costs and expenditures is publicly available at: https://www.boston.gov/departments/budget/fy23-operating-budget and https://www.boston.gov/departments/budget/fy24-operating-budget. Information regarding the Department's FY2023 and FY2024 grant funding is attached. The Department's purchases of surveillance technology are made through the City of Boston procurement process.

The Department does not have any dedicated personnel cost for this technology.

8. **Impact on Communities: Whether the civil rights and liberties of any communities or groups, including communities of color or other marginalized communities in the City, are disproportionately impacted by the deployment of the Surveillance Technology.**

The Boston Police Department strives to maintain the highest standards of honesty and integrity and is committed to building and strengthening trust with all members of the community. *See* BPD Rule 113 (Public Integrity Policy) and BPD Rule 113A (Bias-Free Policing Policy). All members of the Boston Police Department (sworn and civilian) are committed to providing services and enforcing laws in a professional, nondiscriminatory, fair, and equitable manner. This includes services involving the use of this technology. The Boston Police Department is committed to bias-free policing. *See* BPD Rule 113A (Bias-Free Policing Policy).

The Department is not aware of any finding, outcome, or determination of disparate impact involving this technology.

9. **Agreements: A disclosure of any new agreements made in the past 12 months with non-City entities that may include acquiring, sharing, or otherwise using [the] Surveillance Technology or the Surveillance Data it provides.**

In 2023, the Department did not enter into any new agreements with non-City entities to acquire, share, or utilize the technology to expand the Department's capabilities beyond those that have been previously reported.

Department: Boston Police Department
Surveillance Technology: Body Worn Cameras

1. **Description: A description of how [the] Surveillance Technology has been used, including whether it captured images, sound, or other information regarding members of the public who are not suspected of engaging in unlawful conduct.**

Body Worn Cameras (BWCs) are effective law enforcement tools that reinforce the public's perception of police professionalism and preserve factual representations of officer-civilian interactions. BWCs may be useful in documenting crime and accident scenes or other events that include the confiscation and documentation of incidental evidence or contraband. The equipment will enhance the Department's ability to document and review statements and events during the course of an incident, preserve video and audio information and evidence for investigative and prosecutorial purposes.

BWC recordings, however, provide limited perspective of encounters and incidents and must be considered with all other available evidence, such as witnesses' statements, officer interviews, forensic analysis and documentary evidence. Additionally, studies have shown that BWCs are a contributing factor in reducing complaints against police officers, increasing police accountability, and enhancing public trust.

BWCs and software collect data, images, video recordings, audio recordings, and metadata. BWCs are used with Axon View software.

2. **Data Sharing: Whether and how often data acquired through the use of the Surveillance Technology was shared with local, state, and federal [agencies], the name of any recipient entity, the type(s) of data disclosed, any legal standard(s) under which the information was disclosed, and the justification for the disclosure.**

Please see attached spreadsheet for requests the Video Evidence Unit (VEU) received in 2023 to provide BWC video to law enforcement. The VEU received 6,518 requests in 2023.

Federal, state, and local prosecutors shall make requests for BWC footage directly to the Video Evidence Unit. In accordance with current practice, should an officer receive a subpoena for BWC footage, the officer shall direct the subpoena to their supervisor with a Form 26. The officer shall indicate in their Form 26 that a request for video has been made. The officer shall also direct a copy of the subpoena and Form 26 as soon as practicable to the Video Evidence Unit for response.

Officers are not permitted to provide video to any external partners and shall forward any requests made without a subpoena directly to the Video Evidence Unit.

Upon receipt of the request, Video Evidence Unit ("VEU") shall determine if the case has been assigned to a detective. If so, the VEU will notify the assigned Detective and/or Detective Supervisor of the request. The Detective or Detective Supervisor will then be responsible for providing all responsive and related case video directly to the federal, state, or local prosecutor.

If no detective is assigned to the case, VEU shall identify all relevant BWC footage and provide it directly to the federal, state, or local prosecutor.

All requests made from other law enforcement agencies are handled in accordance with all relevant federal and state laws, BPD rules and regulations, including, but not limited to Special Order 21-46 (Outside Agency Notification), and local ordinances including, but not limited to, Chapter 11-1.9 of the City of Boston Municipal Code (Boston Trust Act).

3. Complaints: A summary of community complaints or concerns about the Surveillance Technology, if any.

There were no citizen complaints about the technology.

The Internal Affairs Division identified potential violations of BPD Rule 405 (Body Worn Camera Policy) while investigating citizen complaints unrelated to the surveillance technology in 11 cases. These cases involved the officers' activation of the body worn camera as required by the Rule.

4. Audits: The results of any internal audits, any information about violations of the Surveillance Use Policy, and any actions taken in response other than to the extent that such inclusion would violate the privacy rights of an employee of the City.

All Duty Supervisors assigned to oversee officers utilizing Department-issued BWCs shall:

1. Ensure officers are utilizing their BWC consistent with BPD Rule 405.
2. Ensure BWCs and related equipment are kept in a secure location within the district or unit.
3. Notify the Video Evidence Unit if an officer utilizes a BWC that is not assigned to him or her, so the Unit may reassign the recordings of audio and video to the officer who created the recordings.
4. Contact the Video Evidence Unit whenever any officer is unable to use the BWC or upload digitally recorded data due to technical problems.
5. Request replacement BWC equipment from the Video Evidence Unit when an officer indicates the equipment is lost or malfunctioning via the Special Notification Form. Once procured by Video Evidence Unit ensure new equipment is received by requesting officer.
6. Ensure that officers include all required references to BWCs in appropriate Department documentation, such as incident reports or Form 26 reports.

Duty Supervisors may review BWC data, images, video recordings, audio recordings, or metadata, consistent with BPD Rule 405, to approve any reports. Commanding officers or his/her designee will review BWC activity logs and reports to ensure officers remain in compliance with Department policy and training.

Audits: Audit and Review conducts periodic checks to ensure Department personnel are using BWCs according to Department policy.

The following audits are attached:

- Boston Police Body Worn Camera Performance Audit 2023;

- 2023 Third Quarter Body Worn Camera Compliance Audit; and
- 2023 Fourth Quarter Body Worn Camera Compliance Audit.

During Fiscal Year 2023 (July 1, 2022 through June 20, 2023), approximately 966 Boston Police Officers were randomly selected for body-worn camera review and adherence to BPD Rule 405. The results were as follows:

- Approximately 90% were found to comply with BPD Rule 405.
- Approximately 10% appeared to have deficiencies with BPD Rule 405 (115 total instances).
    - 37 instances: Officers were not recording events.
    - 12 instances: Officers start recordings late or ending recordings early.
    - 19 instances: Officers did not upload video immediately after their tour.
    - 27 instances: Officers were not tagging the video.
    - 20 instances: Officers were not logging into the CAD System.

Discipline: Compliance with all BPD Policies, Procedures, Rules, SOPs, and Special Orders is monitored by the Bureau of Professional Standards, Internal Affairs Division (IAD). *See* BPD Rule 102 (The Conduct and General Responsibilities of Department Personnel) and BPD Rule 109 (Discipline Procedure).

In 2023, there were 16 total IAD investigations that included a potential violation of BPD Rule 405. Each of these allegations are related to an officers' activation of their body worn camera.

5. Effectiveness: A detailed accounting of whether the Surveillance Technology has been effective at achieving its identified purpose.

Body Worn Cameras are effective law enforcement tools that reinforce the public's perception of police professionalism and preserve factual representations of officer-civilian interactions. BWCs are useful in documenting crime and accident scenes or other events that include the confiscation and documentation of incidental evidence or contraband. The equipment enhances the Department's ability to document and review statements and events during the course of an incident, preserve video and audio information and evidence for investigative and prosecutorial purposes. For example:

- On April 27, 2023, officers responded to a radio call for a person shot and located a victim suffering one gunshot wound to his right thigh. Detectives obtained video from residents' cameras, and the BRIC disseminated an ID Wanted bulletin. Responses provided detectives with a person of interest and his address. Detectives utilized databases and learned of a previous 911 call to this address for an incident involving the person of interest; officers with body worn cameras had responded to that incident. Detectives obtained a search warrant to review body camera video footage (Axon Software), which provided evidence that connected the individual to the shooting.

Please see attachment regarding the effectiveness of the Department's surveillance technology for additional information.

6. Public Records Requests: The number of public records requests received by the City seeking documents concerning Surveillance Technologies approved during the previous year.

The Department received 1,135 public records requests for BWC video.

Public records requests often include a request for any and all information relating to the subject of the request. Due to the broad nature of those requests, the responsive documents could potentially include information relative to this technology. With that in mind, and in order to capture all responsive information to this request, the Department received 5,879 public records requests in 2023. A spreadsheet of all the requests is attached.

7. **Cost: An estimate of the total annual costs for the Surveillance Technology, including personnel and other ongoing costs, and what source(s) of funding will fund the technology in the coming year, if known.**

In FY 2023, the Department spent $1,277,442.98.

Information regarding the Department's FY2023 and FY2024 costs and expenditures is publicly available at: https://www.boston.gov/departments/budget/fy23-operating-budget and https://www.boston.gov/departments/budget/fy24-operating-budget. Information regarding the Department's FY2023 and FY2024 grant funding is attached. The Department's purchases of technology are made through the City of Boston procurement process.

The Department does not have any dedicated personnel cost for this technology.

8. **Impact on Communities: Whether the civil rights and liberties of any communities or groups, including communities of color or other marginalized communities in the City, are disproportionately impacted by the deployment of the Surveillance Technology.**

The Boston Police Department strives to maintain the highest standards of honesty and integrity and is committed to building and strengthening trust with all members of the community. *See* BPD Rule 113 (Public Integrity Policy) and BPD Rule 113A (Bias-Free Policing Policy). All members of the Boston Police Department (sworn and civilian) are committed to providing services and enforcing laws in a professional, nondiscriminatory, fair, and equitable manner. This includes services involving the use of this technology. The Boston Police Department is committed to bias-free policing. *See* BPD Rule 113A (Bias-Free Policing Policy).

The Department is not aware of any finding, outcome, or determination of disparate impact involving this technology.

9. **Agreements: A disclosure of any new agreements made in the past 12 months with non-City entities that may include acquiring, sharing, or otherwise using [the] Surveillance Technology or the Surveillance Data it provides.**

In 2023, the Department did not enter into any new agreements with non-City entities to acquire, share, or utilize the technology to expand the Department's capabilities beyond those that have been previously reported.

Attachments:

(a) Video Evidence Unit Requests for BWC Video 2023
(b) Boston Police Body Worn Camera Performance Audit 2023

(c) 2023 Third Quarter Body Worn Camera Compliance Audit [Redacted]
(d) 2023 Fourth Quarter Body Worn Camera Compliance Audit [Redacted]

Department: Boston Police Department
Surveillance Technology: Covert Audio and Video Devices

1. **Description: A description of how [the] Surveillance Technology has been used, including whether it captured images, sound, or other information regarding members of the public who are not suspected of engaging in unlawful conduct.**

The Bureau of Investigative Services (BIS), Special Investigations Unit (SIU) and Drug Control Unit (DCU), the Bureau of Intelligence and Analysis (BIA), Boston Regional Intelligence Center (BRIC), and the Bureau of Field Services (BFS), Youth Violence Strike Force (YVSF) utilize various covert audio and/or video, recording and non-recording devices for legitimate law enforcement purposes and in furtherance of the Department's investigatory, public safety, and community caretaking responsibilities.

Data collection capabilities include: (a) non-recording audio, video, and audio/video; and (b) recording audio, video, and audio/video.

Covert audio and video devices shall only be utilized pursuant to judicial authorization; with valid consent; in exigent circumstances; or in circumstances that do not violate the Fourth Amendment to the United States Constitution or Article 14 of the Massachusetts Declaration of Rights. *See Commonwealth v. Du*, 103 Mass. App. Ct. 469 (2023), further appellate review allowed (SJC-13557); *Commonwealth v. Mora*, 485 Mass. 360 (2020); *see also* BPD Rule 334 (Search Warrant Application and Execution).

2. **Data Sharing: Whether and how often data acquired through the use of the Surveillance Technology was shared with local, state, and federal [agencies], the name of any recipient entity, the type(s) of data disclosed, any legal standard(s) under which the information was disclosed, and the justification for the disclosure.**

Audio and video data (real-time or recorded) captured by covert devices is shared with other law enforcement agencies for legitimate law enforcement purposes only. All requests made from other law enforcement agencies are handled in accordance with all relevant federal and state laws, BPD rules and regulations, including, but not limited to Special Order 21-46 (Outside Agency Notification), and local ordinances including, but not limited to, Chapter 11-1.9 of the City of Boston Municipal Code (Boston Trust Act).

Criminal defendants receive data which is relevant and/or exculpatory to their case through the District Attorney's Office, Attorney General's Office, or United States Attorney's Office pursuant to the rules of discovery, including, but not limited to, Fed. R. Crim. P. 16 and Mass. R. Crim. P. 14, and in accordance with federal and state case law. Additionally, criminal defendants may seek a subpoena or other court order to request the production of specific data pursuant to the rules of criminal procedure, including, but not limited to, Fed. R. Crim. P. 17 and Mass. R. Crim. P. 17.

3. **Complaints: A summary of community complaints or concerns about the Surveillance Technology, if any.**

In an attempt to thoroughly respond to this question, queries were made to the Department's Bureau Chiefs, which includes the Bureau of Field Services, the Bureau of Investigative Services, and the Bureau of Community Engagement, as well as to the individual District Community Service Offices. The Department has not located any specific complaint concerning this technology responsive to this request.

The Department is cognizant that there has been general discussion surrounding the use of technology in the City in various forums and that such discussion may have included complaints or concerns; however, these discussions often occur in forums outside of the Department and, as a result, the Department has been unable to locate any specific complaints relative to this technology.

4. **Audits: The results of any internal audits, any information about violations of the Surveillance Use Policy, and any actions taken in response other than to the extent that such inclusion would violate the privacy rights of an employee of the City.**

Audits: To the extent the technology supports user sign on, the Department utilizes a login with unique identification. All activity is recorded each time an employee logs into the system. All user activity is logged and maintained by the Department, establishing a corresponding audit trail.

Discipline: Compliance with all BPD Policies, Procedures, Rules, SOPs, and Special Orders is monitored by the Bureau of Professional Standards, Internal Affairs Division (IAD). *See* BPD Rule 102 (The Conduct and General Responsibilities of Department Personnel) and BPD Rule 109 (Discipline Procedure).

In 2023, there were 0 IAD complaints with an allegation of misuse of covert audio and video devices.

5. **Effectiveness: A detailed accounting of whether the Surveillance Technology has been effective at achieving its identified purpose.**

In 2023, the Department utilized various covert audio and/or video, recording and non-recording devices for legitimate law enforcement purposes and in furtherance of the Department's investigatory, public safety, and community caretaking responsibilities.

Please see attachment regarding the effectiveness of the Department's surveillance technology.

6. **Public Records Requests: The number of public records requests received by the City seeking documents *concerning* Surveillance Technologies approved during the previous year.**

The Department received 3 requests regarding covert audio and/or video recordings.

Public records requests often include a request for any and all information relating to the subject of the request. Due to the broad nature of those requests, the responsive documents could potentially include information relative to this technology. With that in mind, and in order to capture all responsive information to this request, the Department received 5,879 public records requests in 2023. A spreadsheet of all the requests is attached.

7. **Cost: An estimate of the total annual costs for the Surveillance Technology, including personnel and other ongoing costs, and what source(s) of funding will fund the technology in the coming year, if known.**

Information regarding the Department's FY2023 and FY2024 costs and expenditures is publicly available at: https://www.boston.gov/departments/budget/fy23-operating-budget and https://www.boston.gov/departments/budget/fy24-operating-budget. Information regarding the Department's FY2023 and FY2024 grant funding is attached. The Department's purchases of technology are made through the City of Boston procurement process.

The Department does not have any dedicated personnel cost for this technology.

8. **Impact on Communities: Whether the civil rights and liberties of any communities or groups, including communities of color or other marginalized communities in the City, are disproportionately impacted by the deployment of the Surveillance Technology.**

The Boston Police Department strives to maintain the highest standards of honesty and integrity and is committed to building and strengthening trust with all members of the community. *See* BPD Rule 113 (Public Integrity Policy) and BPD Rule 113A (Bias-Free Policing Policy). All members of the Boston Police Department (sworn and civilian) are committed to providing services and enforcing laws in a professional, nondiscriminatory, fair, and equitable manner. This includes services involving the use of this technology. The Boston Police Department is committed to bias-free policing. *See* BPD Rule 113A (Bias-Free Policing Policy).

The Department is not aware of any finding, outcome, or determination of disparate impact involving this technology.

9. **Agreements: A disclosure of any new agreements made in the past 12 months with non-City entities that may include acquiring, sharing, or otherwise using [the] Surveillance Technology or the Surveillance Data it provides.**

In 2023, the Department did not enter into any new agreements with non-City entities to acquire, share, or utilize the technology to expand the Department's capabilities beyond those that have been previously reported.

Department: Boston Police Department
Surveillance Technology: Specialty Cameras and Devices (Night Vision, Thermal, Infrared, and X-Ray)

1. **Description: A description of how [the] Surveillance Technology has been used, including whether it captured images, sound, or other information regarding members of the public who are not suspected of engaging in unlawful conduct.**

The Boston Police Department Bureau of Investigative Services (BIS), Special Investigations Unit (SIU) and Bureau of Field Services (BFS), Harbor Unit, SWAT, and Special Operations, and Technology Services Division (TSD), Telecommunications Group utilize various specialty cameras and devices for legitimate law enforcement purposes and in furtherance of the Department's investigatory, public safety, and community caretaking responsibilities.

Specialty cameras and devices shall only be utilized pursuant to judicial authorization; with valid consent; in exigent circumstances; or in circumstances that do not violate the Fourth Amendment to the United States Constitution or Article 14 of the Massachusetts Declaration of Rights. *See also* BPD Rule 334 (Search Warrant Application and Execution).

The specialty cameras and devices include the following:
- Night vision cameras: still photographs or real-time video, non-recording
- Thermal imaging cameras: still photographs of recently discarded items, such as firearms; the BAT Camera System (*see* Boston Police Department Cameras and Video Management Systems) is equipped with thermal imaging cameras for viewing heat differential in areas such as Boston Harbor
- Infrared cameras: used by the Harbor Unit to search for individuals or items in the water and do not capture still images or record video
- X-Ray devices: still photographs captured by handheld or robot-mounted devices and used to examine suspicious and unattended items to determine whether explosives are present

2. **Data Sharing: Whether and how often data acquired through the use of the Surveillance Technology was shared with local, state, and federal [agencies], the name of any recipient entity, the type(s) of data disclosed, any legal standard(s) under which the information was disclosed, and the justification for the disclosure.**

Use of the specialty cameras and devices, viewing their images in real-time, and any still photographs or images captured by the devices are shared with other law enforcement agencies for legitimate law enforcement purposes only. All requests made from other law enforcement agencies are handled in accordance with all relevant federal and state laws, BPD rules and regulations, including, but not limited to Special Order 21-46 (Outside Agency Notification), and local ordinances including, but not limited to, Chapter 11-1.9 of the City of Boston Municipal Code (Boston Trust Act).

Criminal defendants receive data which is relevant and/or exculpatory to their case through the District Attorney's Office, Attorney General's Office, or United States Attorney's Office pursuant to the rules of discovery, including, but not limited to, Fed. R. Crim. P. 16 and Mass. R. Crim. P. 14, and in accordance

with federal and state case law. Additionally, criminal defendants may seek a subpoena or other court order to request the production of specific data pursuant to the rules of criminal procedure, including, but not limited to, Fed. R. Crim. P. 17 and Mass. R. Crim. P. 17.

3. **Complaints: A summary of community complaints or concerns about the Surveillance Technology, if any.**

In an attempt to thoroughly respond to this question, queries were made to the Department's Bureau Chiefs, which includes the Bureau of Field Services, the Bureau of Investigative Services, and the Bureau of Community Engagement, as well as to the individual District Community Service Offices. The Department has not located any specific complaint concerning this technology responsive to this request.

4. **Audits: The results of any internal audits, any information about violations of the Surveillance Use Policy, and any actions taken in response other than to the extent that such inclusion would violate the privacy rights of an employee of the City.**

Audits: To the extent the technology supports user sign on, the Department utilizes a login with unique identification. All activity is recorded each time an employee logs into the system. All user activity is logged and maintained by the Department, establishing a corresponding audit trail.

Discipline: Compliance with all BPD Policies, Procedures, Rules, SOPs, and Special Orders is monitored by the Bureau of Professional Standards, Internal Affairs Division (IAD). *See* BPD Rule 102 (The Conduct and General Responsibilities of Department Personnel) and BPD Rule 109 (Discipline Procedure).

In 2023, there were 0 IAD complaints with an allegation of misuse of the specialty cameras and devices.

5. **Effectiveness: A detailed accounting of whether the Surveillance Technology has been effective at achieving its identified purpose.**

In 2023, the Department utilized various specialty cameras and devices for legitimate law enforcement purposes and in furtherance of the Department's investigatory, public safety, and community caretaking responsibilities.

Please see attachment regarding the effectiveness of the Department's surveillance technology.

6. **Public Records Requests: The number of public records requests received by the City seeking documents concerning Surveillance Technologies approved during the previous year.**

The Department did not receive any public records requests regarding specialty cameras or devices.

Public records requests often include a request for any and all information relating to the subject of the request. Due to the broad nature of those requests, the responsive documents could potentially include information relative to this technology. With that in mind, and in order to capture all responsive information to this request, the Department received 5,879 public records requests in 2023. A spreadsheet of all the requests is attached.

7. **Cost: An estimate of the total annual costs for the Surveillance Technology, including personnel and other ongoing costs, and what source(s) of funding will fund the technology in the coming year, if known.**

Information regarding the Department's FY2023 and FY2024 costs and expenditures is publicly available at: https://www.boston.gov/departments/budget/fy23-operating-budget and https://www.boston.gov/departments/budget/fy24-operating-budget. Information regarding the Department's FY2023 and FY2024 grant funding is attached. The Department's purchases of technology are made through the City of Boston procurement process.

The Department does not have any dedicated personnel cost for this technology.

8. **Impact on Communities: Whether the civil rights and liberties of any communities or groups, including communities of color or other marginalized communities in the City, are disproportionately impacted by the deployment of the Surveillance Technology.**

The Boston Police Department strives to maintain the highest standards of honesty and integrity and is committed to building and strengthening trust with all members of the community. *See* BPD Rule 113 (Public Integrity Policy) and BPD Rule 113A (Bias-Free Policing Policy). All members of the Boston Police Department (sworn and civilian) are committed to providing services and enforcing laws in a professional, nondiscriminatory, fair, and equitable manner. This includes services involving the use of this technology. The Boston Police Department is committed to bias-free policing. *See* BPD Rule 113A (Bias-Free Policing Policy).

The Department is not aware of any finding, outcome, or determination of disparate impact involving this technology.

9. **Agreements: A disclosure of any new agreements made in the past 12 months with non-City entities that may include acquiring, sharing, or otherwise using [the] Surveillance Technology or the Surveillance Data it provides.**

In 2023, the Department did not enter into any new agreements with non-City entities to acquire, share, or utilize the technology to expand the Department's capabilities beyond those that have been previously reported.

Department: Boston Police Department
Surveillance Technology: Gunshot Detection Technology, SoundThinking ShotSpotter (Outdoors and Audio Only)

1. **Description: A description of how [the] Surveillance Technology has been used, including whether it captured images, sound, or other information regarding members of the public who are not suspected of engaging in unlawful conduct.**

The City of Boston is an existing end-user customer of SoundThinking's ShotSpotter gunshot location and detection system, which is provided on a software as a service, subscription basis.

The acoustic sensors capture audio recordings of gunshots or suspected gunshots. Each acoustic sensor captures the precise time and audio associated with impulsive sounds that may represent gunfire. This data is used to locate the incident and is then filtered by sophisticated machine algorithms to classify the event as a potential gunshot.

The sensors are triggered and an incident is created only when 3 or more sensors hear the same loud impulsive sound and can verify a location. This creates an incident and sends a short audio snippet to the ShotSpotter Incident Review center. The snippet includes the gunfire and 1 second of audio prior to and after the gunfire to establish an ambient noise level. Audio clips are typically only a few seconds long.

Real-time notifications of gunfire incidents include the following data: incident location (dot on the map); type of gunfire (single round, multiple round); unique identification number; date and time of the muzzle blast (trigger time); nearest address of the gunfire location; number of shots; district identification; and beat identification. The real-time notification also includes a link to the audio snippet, which is valid for 24 hours.

No personally identifiable information is associated with a real-time notification.

2. **Data Sharing: Whether and how often data acquired through the use of the Surveillance Technology was shared with local, state, and federal [agencies], the name of any recipient entity, the type(s) of data disclosed, any legal standard(s) under which the information was disclosed, and the justification for the disclosure.**

All requests made from other law enforcement agencies are handled in accordance with all relevant federal and state laws, BPD rules and regulations, including, but not limited to Special Order 21-46 (Outside Agency Notification), and local ordinances including, but not limited to, Chapter 11-1.9 of the City of Boston Municipal Code (Boston Trust Act).

Criminal defendants receive surveillance data which is relevant and/or exculpatory to their case through the District Attorney's Office, Attorney General's Office, or United States Attorney's Office pursuant to the rules of discovery, including, but not limited to, Fed. R. Crim. P. 16 and Mass. R. Crim. P. 14, and in accordance with federal and state case law. Additionally, criminal defendants may seek a subpoena or other court order to request the production of specific data pursuant to the rules of criminal procedure, including, but not limited to, Fed. R. Crim. P. 17 and Mass. R. Crim. P. 17.

3. **Complaints: A summary of community complaints or concerns about the Surveillance Technology, if any.**

In an attempt to thoroughly respond to this question, queries were made to the Department's Bureau Chiefs, which includes the Bureau of Field Services, the Bureau of Investigative Services, and the Bureau of Community Engagement, as well as to the individual District Community Service Offices. The Department has not located any specific complaint concerning this technology responsive to this request.

The Department is cognizant that there has been general discussion surrounding the use of technology in the City in various forums and that such discussion may have included complaints or concerns; however, these discussions often occur in forums outside of the Department and, as a result, the Department has been unable to locate any specific complaints relative to this technology.

On the contrary, the Department received feedback from community members who do not have ShotSpotter coverage. Residential and business community members have requested additional ShotSpotter coverage in more neighborhoods throughout the City.

4. **Audits: The results of any internal audits, any information about violations of the Surveillance Use Policy, and any actions taken in response other than to the extent that such inclusion would violate the privacy rights of an employee of the City.**

Audits: To the extent the technology supports user sign on, the Department utilizes a login with unique identification. All activity is recorded each time an employee logs into the system. All user activity is logged and maintained by the Department, establishing a corresponding audit trail.

The Department publishes datasets regarding confirmed shots fired and persons shot.

Confirmed Shots Fired:
https://boston.hub.arcgis.com/datasets/dd3a722ccc964876b0c6f426541d704d/explore

Persons shot: https://boston.hub.arcgis.com/datasets/boston::person-shot/explore

Discipline: Compliance with all BPD Policies, Procedures, Rules, SOPs, and Special Orders is monitored by the Bureau of Professional Standards, Internal Affairs Division (IAD). *See* BPD Rule 102 (The Conduct and General Responsibilities of Department Personnel) and BPD Rule 109 (Discipline Procedure).

In 2023, there were 0 IAD complaints with an allegation of misuse of the ShotSpotter system or data.

5. **Effectiveness: A detailed accounting of whether the Surveillance Technology has been effective at achieving its identified purpose.**

ShotSpotter serves as an acoustical technology that precisely locates the area where gunshots have been fired and provides immediate alert/notification. On average, notifications arrive one to two minutes before 911 calls.

For example:

- In February 2023, RTCC Analysts responded to a ShotSpotter activation for 4 rounds on Seaver St., followed by a call for shots fired at Elm Hill Ave. / Seaver St., later upgraded to a person shot. The victim was located suffering from a graze wound to his left ankle; he provided a description of two suspects. RTCC Analysts utilized the BAT Camera System and observed two individuals who appeared to be shooting at the victim's vehicle. RTCC Analysts confirmed the suspects' descriptions and direction of flight to BPD Operations and disseminated a screenshot of the suspects to units in the field.

Sometimes, notifications arrive without a 911 call. This state-of-the-art program and enhanced response time better enables the Department to identify hotspots, recover evidence, and locate both victims and people in possession of guns.

In 2023, in two separate incidents, officers located two shooting victims when they responded to ShotSpotter alerts and arrived on scenes where otherwise there were no 911 calls made.

In fact, in 2023, about 40% of confirmed shots fired incidents inside the ShotSpotter coverage zone where ShotSpotter activated did not have a corresponding 911 call. This was calculated by taking the total number of unique gunfire incidents within the ShotSpotter coverage area where a ShotSpotter alert was issued and ballistics were recovered and reviewing whether there was a corresponding, near contemporaneous 911 call to the best of our abilities. The total number of confirmed shots fired in the coverage area without a 911 call was divided by the overall total number of confirmed shots fired in the coverage area (75 / 187).

For example:

- In February 2023, officers responded to a ShotSpotter activation for 13 rounds on Dale Street. There were no 911 calls made in relation to this incident. While officers were on scene, they utilized the ShotSpotter application and saw ballistic evidence was potentially located inside of Malcolm X Park. On an unpaved dirt pathway inside the park, officers located 13 spent shell casings. After extensive investigation, detectives identified the shooter and a warrant was issued for his arrest.
- In May 2023, officers responded to a ShotSpotter activation in the South End with no corresponding 911 calls. After further investigation, including review of Surveillance Video, 3 individuals were arrested on firearms related charges. Evidence indicates the firearm used in this incident was likely connected to three additional shots fired incidents in Boston.
- In June 2023, around 5:00 a.m., officers responded to a ShotSpotter activation near Bellevue Street. There were no 911 calls. Officers located ballistic evidence and a suspect. After further investigation, and following the execution of a search warrant, a ghost gun was recovered and the suspect was arrested.
- In August 2023, around 11:00 a.m., officers responded to a ShotSpotter activation for 12 rounds of gunfire on Codman Park. There were no 911 calls. At the scene, 12 shell casings were recovered and a victim provided descriptions of the two individuals who shot at him. Investigators reviewed private surveillance camera footage and broadcast descriptions of the two shooters. Within an hour, two suspects were arrested and an unattended firearm was recovered.
- In October 2023, officers responded to a ShotSpotter activation for 6 rounds near Castlegate Road. No corresponding 911 calls were received. Officers were unable to locate any victim(s), witnesses, or ballistic evidence on scene. After additional investigation, and less than an hour

later, officers conducted a protective sweep of a basement and located two firearms in a common laundry area. One firearm was loaded with a round in the chamber and 24 rounds in a 30 round magazine.

- In October 2023, a suspect was arrested and ghost gun recovered following a ShotSpotter activation on Topliff St. There were no 911 calls. The suspect was apprehended operating a motor scooter fleeing the scene.

Please see attachment regarding the effectiveness of the Department's surveillance technology for additional information.

6. **Public Records Requests: The number of public records requests received by the City seeking documents concerning Surveillance Technologies approved during the previous year.**

The Department received 10 public records requests for records specifically regarding ShotSpotter.

Public records requests often include a request for any and all information relating to the subject of the request. Due to the broad nature of those requests, the responsive documents could potentially include information relative to this technology. With that in mind, and in order to capture all responsive information to this request, the Department received 5,879 public records requests in 2023, including the 10 requests specifically regarding ShotSpotter. A spreadsheet of all the requests is attached.

7. **Cost: An estimate of the total annual costs for the Surveillance Technology, including personnel and other ongoing costs, and what source(s) of funding will fund the technology in the coming year, if known.**

In FY 2023, the Department spent $260,664.00. Additionally, in 2023, the Department added 2 square miles of coverage that was purchased using Urban Area Security Initiative (UASI) federal grant funding. A copy of the contract amendment is attached. The contract amendment cost an additional $37,274.00 (this cost includes fees for the 2.0 square mile expansion, which will be prorated from the date of service activation, estimated to be December 31, 2023, to January 31, 2024).

Information regarding the Department's FY2023 and FY2024 costs and expenditures is publicly available at: https://www.boston.gov/departments/budget/fy23-operating-budget and https://www.boston.gov/departments/budget/fy24-operating-budget. Information regarding the Department's FY2023 and FY2024 grant funding is attached. The Department's purchases of technology are made through the City of Boston procurement process.

The Department does not have any dedicated personnel cost for this technology.

8. **Impact on Communities: Whether the civil rights and liberties of any communities or groups, including communities of color or other marginalized communities in the City, are disproportionately impacted by the deployment of the Surveillance Technology.**

The Boston Police Department strives to maintain the highest standards of honesty and integrity and is committed to building and strengthening trust with all members of the community. *See* BPD Rule 113 (Public Integrity Policy) and BPD Rule 113A (Bias-Free Policing Policy). All members of the Boston Police Department (sworn and civilian) are committed to providing services and enforcing laws in a

professional, nondiscriminatory, fair, and equitable manner. The Boston Police Department is committed to bias-free policing. BPD Rule 113A (Bias-Free Policing Policy).

9. **Agreements: A disclosure of any new agreements made in the past 12 months with non-City entities that may include acquiring, sharing, or otherwise using [the] Surveillance Technology or the Surveillance Data it provides.**

In 2023, the City contracted for an additional 2 square miles of ShotSpotter coverage, which is paid for through the UASI funding. A copy of the contract amendment is attached.

Attachments:

(a) City of Boston / OEM Agreement with SoundThinking, Inc. for Additional ShotSpotter Coverage

Department: Boston Police Department
Surveillance Technology: Cell-Site Simulator

1. **Description: A description of how [the] Surveillance Technology has been used, including whether it captured images, sound, or other information regarding members of the public who are not suspected of engaging in unlawful conduct.**

The Boston Police Department Bureau of Investigative Services (BIS) utilizes a cell-site simulator to locate or identify mobile devices by the device's industry-standard unique-identifying number, such as the International Mobile Equipment Identity (IMEI) number.

The technology is used to locate missing persons, victims of crimes, such as abductions, and criminal suspects. The cell-site simulator is used only for legitimate law enforcement purposes and in furtherance of the Department's investigatory, public safety, and community caretaking responsibilities.

The cell-site simulator is used (1) with a search warrant obtained after a judicial finding of probable cause; or (2) in exigent circumstances.

Cell-site simulators acquire limited information from cellular devices.[1] Cell-site simulators provide only the relative signal strength and general direction of a cellular device; they do not function as a global positioning locator.

The cell-site simulator cannot collect the contents of any communication or any data contained on the device itself. The cell-site simulator cannot capture emails, texts, contact lists, images or any other data from the device, nor do they provide subscriber account information (for example, an account holder's name, address, or telephone number). Cell-site simulators do not use any biometric measuring technologies.

The cell-site simulator is used in conjunction with vendor-provided software. The associated software displays the location data processed by the cell-site simulator in a format usable by BPD personnel. Data or information will not be retained unless court ordered by a judge.

2. **Data Sharing: Whether and how often data acquired through the use of the Surveillance Technology was shared with local, state, and federal [agencies], the name of any recipient entity,**

[1] Cell-site simulators function by behaving like a traditional networked cell tower. In response to signals emitted by a cell-site simulator, cellular devices within the proximity of the cell-site simulator identify it as the most attractive cell tower in the area. When the simulator is within the cellular device's signal range, it measures the device's signal strength and general direction of the phone. Every device capable of connecting to a cellular network through a cell tower is assigned an industry-standard unique-identifying number by the device's manufacturer or cellular network provider. Cell-site simulators are used either (a) to locate a cellular device where the unique-identifying number is known or (b) to identify a cellular device with an unknown unique-identifying number by deploying the cell-site simulator at several locations where an individual is known to be present and then identifying the unique-identifying number which is present at each of the locations.

the type(s) of data disclosed, any legal standard(s) under which the information was disclosed, and the justification for the disclosure.

No external entities have access to the BPD cell-site simulator or associated software. This does not prohibit mutual aid or assistance requests by other law enforcement agencies that have been approved by the Commander of the SIU and BIS Command.

All requests made from other law enforcement agencies are handled in accordance with all relevant federal and state laws, BPD rules and regulations, including, but not limited to Special Order 21-46 (Outside Agency Notification), and local ordinances including, but not limited to, Chapter 11-1.9 of the City of Boston Municipal Code (Boston Trust Act).

In 2023, the Department received 0 mutual aid or data sharing requests from other law enforcement agencies.

3. **Complaints: A summary of community complaints or concerns about the Surveillance Technology, if any.**

In an attempt to thoroughly respond to this question, queries were made to the Department's Bureau Chiefs, which includes the Bureau of Field Services, the Bureau of Investigative Services, and the Bureau of Community Engagement, as well as to the individual District Community Service Offices. The Department has not located any specific complaint concerning this technology responsive to this request.

The Department is cognizant that there has been general discussion surrounding the use of technology in the City in various forums and that such discussion may have included complaints or concerns; however, these discussions often occur in forums outside of the Department and, as a result, the Department has been unable to locate any specific complaints relative to this technology.

4. **Audits: The results of any internal audits, any information about violations of the Surveillance Use Policy, and any actions taken in response other than to the extent that such inclusion would violate the privacy rights of an employee of the City.**

Audits: The BPD Investigator or Supervisor requesting to utilize the cell-site simulator must discuss the reasons for deployment with the Commander of SIU and/or BIS Command. Only SIU personnel can operate the cell-site simulator, which may only be done after receiving proper approvals, including a search warrant where exigent circumstances do not exist. A cell-site simulator will not be used without proper internal approvals, even in exigent circumstances.

During 2023, each use of the cell-site simulator followed this protocol.

Discipline: Compliance with all BPD Policies, Procedures, Rules, SOPs, and Special Orders is monitored by the Bureau of Professional Standards, Internal Affairs Division (IAD). *See* BPD Rule 102 (The Conduct and General Responsibilities of Department Personnel) and BPD Rule 109 (Discipline Procedure). The misuse of the cell-site simulator or associated software will subject employees to administrative and potentially criminal penalties. Allegations of misuse are internally investigated at the command level or by IAD.

In 2023, neither IAD nor the Commander of SIU received any information regarding misuse of the cell-site simulator or data.

5. **Effectiveness: A detailed accounting of whether the Surveillance Technology has been effective at achieving its identified purpose.**

Please see attachment regarding the effectiveness of the Department's surveillance technology.

In 2023, the cell-site simulator was used in furtherance of the Department's investigatory, public safety and community caretaking responsibilities. One one occasion, the equipment was used during an investigation and resulted in the apprehension of an individual wanted on an outstanding arrest warrant for armed robbery. During an unrelated investigation, the equipment was used to confirm the location of a suspect in an aggravated assault incident.

6. **Public Records Requests: The number of public records requests received by the City seeking documents concerning Surveillance Technologies approved during the previous year.**

The Department received 0 public records requests for the cell-site simulator technology or data.

Public records requests often include a request for any and all information relating to the subject of the request. Due to the broad nature of those requests, the responsive documents could potentially include information relative to this technology. With that in mind, and in order to capture all responsive information to this request, the Department received 5,879 public records requests in 2023. A spreadsheet of all the requests is attached.

7. **Cost: An estimate of the total annual costs for the Surveillance Technology, including personnel and other ongoing costs, and what source(s) of funding will fund the technology in the coming year, if known.**

Information regarding the Department's FY2023 and FY2024 costs and expenditures is publicly available at: https://www.boston.gov/departments/budget/fy23-operating-budget and https://www.boston.gov/departments/budget/fy24-operating-budget. Information regarding the Department's FY2023 and FY2024 grant funding is attached. The Department's purchases of technology are made through the City of Boston procurement process.

The Department does not have any dedicated personnel cost for this technology.

8. **Impact on Communities: Whether the civil rights and liberties of any communities or groups, including communities of color or other marginalized communities in the City, are disproportionately impacted by the deployment of the Surveillance Technology.**

The Boston Police Department strives to maintain the highest standards of honesty and integrity and is committed to building and strengthening trust with all members of the community. *See* BPD Rule 113 (Public Integrity Policy) and BPD Rule 113A (Bias-Free Policing Policy). All members of the Boston Police Department (sworn and civilian) are committed to providing services and enforcing laws in a professional, nondiscriminatory, fair, and equitable manner. This includes services involving the use of

this technology. The Boston Police Department is committed to bias-free policing. *See* BPD Rule 113A (Bias-Free Policing Policy).

The Department is not aware of any finding, outcome, or determination of disparate impact involving this technology.

9. **Agreements: A disclosure of any new agreements made in the past 12 months with non-City entities that may include acquiring, sharing, or otherwise using [the] Surveillance Technology or the Surveillance Data it provides.**

In 2023, the Department did not enter into any new agreements with non-City entities to acquire, share, or utilize the technology to expand the Department's capabilities beyond those that have been previously reported.

Department: Boston Police Department
Surveillance Technology: GPS Tracking Units

1. **Description: A description of how [the] Surveillance Technology has been used, including whether it captured images, sound, or other information regarding members of the public who are not suspected of engaging in unlawful conduct.**

The Boston Police Department Bureau of Field Services, Bureau of Investigative Services, and Bureau of Intelligence & Analysis utilize Global Positioning System (GPS) trackers to track the movements and precise location of vehicles, cargo, machinery, and/or individuals. GPS trackers are used for legitimate law enforcement purposes only, and primarily, the investigation of criminal activity, including, but not limited to, investigations into sophisticated drug trafficking organizations, human trafficking investigations, and investigations into organized crime and violent street gangs.

GPS trackers only transmit encrypted data (*i.e.*, movement tracking and location data), which allows authorized BPD personnel to monitor the device's location in real-time. GPS tracker data is also electronically recorded and stored in individual case files.

GPS trackers shall only be utilized pursuant to judicial authorization; with valid consent; in exigent circumstances; or in circumstances that do not violate the Fourth Amendment to the United States Constitution or Article 14 of the Massachusetts Declaration of Rights. Consistent with Article 14 of the Massachusetts Declaration of Rights, a warrant application seeking to install a GPS device on a target vehicle, must establish "probable cause to believe that a particularly described offense has been, is being, or is about to be committed, and that GPS monitoring of the vehicle will produce evidence of such offense or will aid in the apprehension of a person who the applicant has probable cause to believe has committed, is committing, or is about to commit such offense." *See Commonwealth v. Connolly*, 454 Mass. 808, 825 (2009); *see also* BPD Rule 334 (Search Warrant Application and Execution).

2. **Data Sharing: Whether and how often data acquired through the use of the Surveillance Technology was shared with local, state, and federal [agencies], the name of any recipient entity, the type(s) of data disclosed, any legal standard(s) under which the information was disclosed, and the justification for the disclosure.**

No outside agencies (City or non-City entities) have direct access to the Department's GPS data.

GPS data is shared with other law enforcement agencies for legitimate law enforcement purposes only. All requests made from other law enforcement agencies are handled in accordance with all relevant federal and state laws, BPD rules and regulations, including, but not limited to, Special Order 21-46 (Outside Agency Notification), and local ordinances including, but not limited to, Chapter 11-1.9 of the City of Boston Municipal Code (Boston Trust Act).

Criminal defendants receive data which is relevant and/or exculpatory to their case through the District Attorney's Office, Attorney General's Office, or United States Attorney's Office pursuant to the rules of discovery, including, but not limited to, Fed. R. Crim. P. 16 and Mass. R. Crim. P. 14, and in accordance with federal and state case law. Additionally, criminal defendants may seek a subpoena or other court

order to request the production of specific data pursuant to the rules of criminal procedure, including, but not limited to, Fed. R. Crim. P. 17 and Mass. R. Crim. P. 17.

3. **Complaints: A summary of community complaints or concerns about the Surveillance Technology, if any.**

In an attempt to thoroughly respond to this question, queries were made to the Department's Bureau Chiefs, which includes the Bureau of Field Services, the Bureau of Investigative Services, and the Bureau of Community Engagement, as well as to the individual District Community Service Offices. The Department has not located any specific complaint concerning this technology responsive to this request.

4. **Audits: The results of any internal audits, any information about violations of the Surveillance Use Policy, and any actions taken in response other than to the extent that such inclusion would violate the privacy rights of an employee of the City.**

Audits: To the extent the technology supports user sign on, the Department utilizes a login with unique identification. All activity is recorded each time an employee logs into the system. All user activity is logged and maintained by the Department, establishing a corresponding audit trail.

Discipline: Compliance with all BPD Policies, Procedures, Rules, SOPs, and Special Orders is monitored by the Bureau of Professional Standards, Internal Affairs Division (IAD). *See* BPD Rule 102 (The Conduct and General Responsibilities of Department Personnel) and BPD Rule 109 (Discipline Procedure).

In 2023, there were 0 IAD complaints with an allegation of misuse of GPS tracking devices or data.

5. **Effectiveness: A detailed accounting of whether the Surveillance Technology has been effective at achieving its identified purpose.**

GPS trackers are used for legitimate law enforcement purposes only, and primarily, the investigation of criminal activity, including, but not limited to, investigations into sophisticated drug trafficking organizations, human trafficking investigations, and investigations into organized crime and violent street gangs.

Please see attachment regarding the effectiveness of the Department's surveillance technology.

6. **Public Records Requests: The number of public records requests received by the City seeking documents concerning Surveillance Technologies approved during the previous year.**

The Department received 1 public records request for GPS Tracking Unit information/data.

Public records requests often include a request for any and all information relating to the subject of the request. Due to the broad nature of those requests, the responsive documents could potentially include information relative to this technology. With that in mind, and in order to capture all responsive information to this request, the Department received 5,879 public records requests in 2023. A spreadsheet of all the requests is attached.

7. **Cost: An estimate of the total annual costs for the Surveillance Technology, including personnel and other ongoing costs, and what source(s) of funding will fund the technology in the coming year, if known.**

Information regarding the Department's FY2023 and FY2024 costs and expenditures is publicly available at: https://www.boston.gov/departments/budget/fy23-operating-budget and https://www.boston.gov/departments/budget/fy24-operating-budget. Information regarding the Department's FY2023 and FY2024 grant funding is attached. The Department's purchases of technology are made through the City of Boston procurement process.

The Department does not have any dedicated personnel cost for this technology.

8. **Impact on Communities: Whether the civil rights and liberties of any communities or groups, including communities of color or other marginalized communities in the City, are disproportionately impacted by the deployment of the Surveillance Technology.**

The Boston Police Department strives to maintain the highest standards of honesty and integrity and is committed to building and strengthening trust with all members of the community. *See* BPD Rule 113 (Public Integrity Policy) and BPD Rule 113A (Bias-Free Policing Policy). All members of the Boston Police Department (sworn and civilian) are committed to providing services and enforcing laws in a professional, nondiscriminatory, fair, and equitable manner. This includes services involving the use of this technology. The Boston Police Department is committed to bias-free policing. *See* BPD Rule 113A (Bias-Free Policing Policy).

The Department is not aware of any finding, outcome, or determination of disparate impact involving this technology.

9. **Agreements: A disclosure of any new agreements made in the past 12 months with non-City entities that may include acquiring, sharing, or otherwise using [the] Surveillance Technology or the Surveillance Data it provides.**

In 2023, the Department did not enter into any new agreements with non-City entities to acquire, share, or utilize the technology to expand the Department's capabilities beyond those that have been previously reported.

Department: Boston Police Department
Surveillance Technology: Electronic Intercept & Analysis System ("Wire Room")

1. **Description: A description of how [the] Surveillance Technology has been used, including whether it captured images, sound, or other information regarding members of the public who are not suspected of engaging in unlawful conduct.**

The Boston Police Department Bureau of Investigative Services, Special Investigations Unit utilizes an Electronic Intercept & Analysis System (the "System"), colloquially known as a "Wire Room," to gather evidence of a crime and intelligence about suspected criminal activity conducted by an individual(s) or organized group through interception of wire, oral, or electronic communications.

All data and records collected by the System are obtained by a legal demand, such as an administrative subpoena, search warrant, and court order, and pursuant to federal and state law, including, but not limited to 18 U.S.C. § 2518 and G.L. ch. 272, § 99. *See also* BPD Rule 334 (Search Warrant Application and Execution). On occasion, limited records are obtained as a result of exigent circumstances.

Surveillance data collected by the System include wire, oral, and electronic communications. The specific categories and types of data and records that are collected are determined based on the investigation and are enumerated in the search warrant or court order with the requisite articulation of the probable cause in support of collecting the data pursuant to 18 U.S.C. § 2518 and G.L. ch. 272, § 99.

2. **Data Sharing: Whether and how often data acquired through the use of the Surveillance Technology was shared with local, state, and federal [agencies], the name of any recipient entity, the type(s) of data disclosed, any legal standard(s) under which the information was disclosed, and the justification for the disclosure.**

Access to the data collected is restricted by federal and state law. Data is only shared if the entity is involved in the specific investigation and pursuant to court order or otherwise required by law.

All requests made from other law enforcement agencies are handled in accordance with all relevant federal and state laws, BPD rules and regulations, including, but not limited to Special Order 21-46 (Outside Agency Notification), and local ordinances including, but not limited to, Chapter 11-1.9 of the City of Boston Municipal Code (Boston Trust Act).

Criminal defendants receive data which is relevant and/or exculpatory to their case through the District Attorney's Office, Attorney General's Office, or United States Attorney's Office pursuant to the rules of discovery, including, but not limited to, Fed. R. Crim. P. 16 and Mass. R. Crim. P. 14, and in accordance with federal and state case law. Additionally, criminal defendants may seek a subpoena or other court order to request the production of specific data pursuant to the rules of criminal procedure, including, but not limited to, Fed. R. Crim. P. 17 and Mass. R. Crim. P. 17.

3. **Complaints: A summary of community complaints or concerns about the Surveillance Technology, if any.**

In an attempt to thoroughly respond to this question, queries were made to the Department's Bureau Chiefs, which includes the Bureau of Field Services, the Bureau of Investigative Services, and the Bureau of Community Engagement, as well as to the individual District Community Service Offices. The Department has not located any specific complaint concerning this technology responsive to this request.

4. **Audits: The results of any internal audits, any information about violations of the Surveillance Use Policy, and any actions taken in response other than to the extent that such inclusion would violate the privacy rights of an employee of the City.**

Audits: Security protocols and internal audits are monitored and managed by the System Administrator.

Discipline: Compliance with all BPD Policies, Procedures, Rules, SOPs, and Special Orders is monitored by the Bureau of Professional Standards, Internal Affairs Division (IAD). *See* BPD Rule 102 (The Conduct and General Responsibilities of Department Personnel) and BPD Rule 109 (Discipline Procedure).

In 2023, there were 0 IAD complaints with an allegation of misuse of the Wire Room.

5. **Effectiveness: A detailed accounting of whether the Surveillance Technology has been effective at achieving its identified purpose.**

The Wire Room is used to develop evidence of a crime and intelligence about suspected criminal activity conducted by an individual(s) or organized group through interception of wire, oral, or electronic communications.

Please see attachment regarding the effectiveness of the Department's surveillance technology.

6. **Public Records Requests: The number of public records requests received by the City seeking documents concerning Surveillance Technologies approved during the previous year.**

The Department received 0 public records requests for information/documents related to the Wire Room.

Public records requests often include a request for any and all information relating to the subject of the request. Due to the broad nature of those requests, the responsive documents could potentially include information relative to this technology. With that in mind, and in order to capture all responsive information to this request, the Department received 5,879 public records requests in 2023. A spreadsheet of all the requests is attached.

7. **Cost: An estimate of the total annual costs for the Surveillance Technology, including personnel and other ongoing costs, and what source(s) of funding will fund the technology in the coming year, if known.**

Information regarding the Department's FY2023 and FY2024 costs and expenditures is publicly available at: https://www.boston.gov/departments/budget/fy23-operating-budget and

https://www.boston.gov/departments/budget/fy24-operating-budget. Information regarding the Department's FY2023 and FY2024 grant funding is attached. The Department's purchases of technology are made through the City of Boston procurement process.

The Department does not have any dedicated personnel cost for this technology.

8. **Impact on Communities: Whether the civil rights and liberties of any communities or groups, including communities of color or other marginalized communities in the City, are disproportionately impacted by the deployment of the Surveillance Technology.**

The Boston Police Department strives to maintain the highest standards of honesty and integrity and is committed to building and strengthening trust with all members of the community. *See* BPD Rule 113 (Public Integrity Policy) and BPD Rule 113A (Bias-Free Policing Policy). All members of the Boston Police Department (sworn and civilian) are committed to providing services and enforcing laws in a professional, nondiscriminatory, fair, and equitable manner. This includes services involving the use of this technology. The Boston Police Department is committed to bias-free policing. *See* BPD Rule 113A (Bias-Free Policing Policy).

The Department is not aware of any finding, outcome, or determination of disparate impact involving this technology.

9. **Agreements**: A disclosure of any new agreements made in the past 12 months with non-City entities that may include acquiring, sharing, or otherwise using [the] Surveillance Technology or the Surveillance Data it provides.

In 2023, the Department did not enter into any new agreements with non-City entities to acquire, share, or utilize the technology to expand the Department's capabilities beyond those that have been previously reported.

Department: Boston Police Department
Surveillance Technology: Forensic Examination Hardware and Software

1. **Description: A description of how [the] Surveillance Technology has been used, including whether it captured images, sound, or other information regarding members of the public who are not suspected of engaging in unlawful conduct.**

Electronic Crimes Investigators assigned to the Boston Police Department Forensic Group utilize hardware and software to conduct forensic examinations of handheld devices, computers, and other electronic equipment, including:

- Mobile devices - Smartphones, Tablets, etc.
- Storage devices - Thumb Drives, External Hard Drives, SD Cards/MicroSD
- Computers - Macintosh and Windows
- Network Intrusion Response/Malware Analysis
- Vehicle System Forensics - Infotainment and Telematics Systems
- Skimmer Forensics
- Drone Forensics

Investigators also utilize tools to provide support for Cyber Crime Investigations.

The tools have the potential to access a wide range of data on digital devices, including personal and sensitive information. The data retrieved using the tools and software includes computer files, e-mails, contacts, digital images, audio and video files, and other multimedia files.

All forensic examinations are conducted in furtherance of legitimate law enforcement purposes. Examinations are conducted in criminal investigations with consent or pursuant to a court order. *See* BPD Rule 334 (Search Warrant Application and Execution). Examinations may also be necessary in exigent circumstances. The Department does not use any "[t]ools, including software or hardware, to gain unauthorized access to a computer, computer service, or computer network" -- or any electronic device.

2. **Data Sharing: Whether and how often data acquired through the use of the Surveillance Technology was shared with local, state, and federal [agencies], the name of any recipient entity, the type(s) of data disclosed, any legal standard(s) under which the information was disclosed, and the justification for the disclosure.**

No other agency has direct access to BPD forensic hardware/software or associated surveillance data. This does not prohibit mutual aid or assistance requests by other law enforcement agencies. All requests made from other law enforcement agencies are handled in accordance with all relevant federal and state laws, BPD rules and regulations, including, but not limited to Special Order 21-46 (Outside Agency Notification), and local ordinances including, but not limited to, Chapter 11-1.9 of the City of Boston Municipal Code (Boston Trust Act).

Criminal defendants receive data which is relevant and/or exculpatory to their case through the District Attorney's Office, Attorney General's Office, or United States Attorney's Office pursuant to the rules of discovery, including, but not limited to, Fed. R. Crim. P. 16 and Mass. R. Crim. P. 14, and in accordance with federal and state case law. Additionally, criminal defendants may seek a subpoena or other court order to request the production of specific data pursuant to the rules of criminal procedure, including, but not limited to, Fed. R. Crim. P. 17 and Mass. R. Crim. P. 17.

3. **Complaints: A summary of community complaints or concerns about the Surveillance Technology, if any.**

In an attempt to thoroughly respond to this question, queries were made to the Department's Bureau Chiefs, which includes the Bureau of Field Services, the Bureau of Investigative Services, and the Bureau of Community Engagement, as well as to the individual District Community Service Offices. The Department has not located any specific complaint concerning this technology responsive to this request.

4. **Audits: The results of any internal audits, any information about violations of the Surveillance Use Policy, and any actions taken in response other than to the extent that such inclusion would violate the privacy rights of an employee of the City.**

Audits: To the extent the technology supports user sign on, the Department utilizes a login with unique identification. All activity is recorded each time an employee logs into the system. All user activity is logged and maintained by the Department, establishing a corresponding audit trail. When the data extraction/examination forensic tools and software have embedded audit features, the Department shall conduct audits as it deems necessary to ensure appropriate use of the forensic tools and software.

Discipline: Compliance with all BPD Policies, Procedures, Rules, SOPs, and Special Orders is monitored by the Bureau of Professional Standards, Internal Affairs Division. *See* BPD Rule 102 (The Conduct and General Responsibilities of Department Personnel) and BPD Rule 109 (Discipline Procedure).

In 2023, there were 0 IAD complaints with an allegation of misuse of forensic examination hardware or software.

5. **Effectiveness: A detailed accounting of whether the Surveillance Technology has been effective at achieving its identified purpose.**

Electronic Crimes Investigators assigned to the Boston Police Department Forensic Group utilize hardware and software to conduct forensic examinations of handheld devices, computers, and other electronic equipment in furtherance of legitimate law enforcement purposes.

Please see attachment regarding the effectiveness of the Department's surveillance technology.

6. **Public Records Requests: The number of public records requests received by the City seeking documents concerning Surveillance Technologies approved during the previous year.**

The Department received 5 public records requests that included a request for forensic examination records.

Public records requests often include a request for any and all information relating to the subject of the request. Due to the broad nature of those requests, the responsive documents could potentially include information relative to this technology. With that in mind, and in order to capture all responsive information to this request, the Department received 5,879 public records requests in 2023. A spreadsheet of all the requests is attached.

7. **Cost: An estimate of the total annual costs for the Surveillance Technology, including personnel and other ongoing costs, and what source(s) of funding will fund the technology in the coming year, if known.**

Information regarding the Department's FY2023 and FY2024 costs and expenditures is publicly available at: https://www.boston.gov/departments/budget/fy23-operating-budget and https://www.boston.gov/departments/budget/fy24-operating-budget. Information regarding the Department's FY2023 and FY2024 grant funding is attached. The Department's purchases of technology are made through the City of Boston procurement process.

The Department does not have any dedicated personnel cost for this technology.

8. **Impact on Communities: Whether the civil rights and liberties of any communities or groups, including communities of color or other marginalized communities in the City, are disproportionately impacted by the deployment of the Surveillance Technology.**

The Boston Police Department strives to maintain the highest standards of honesty and integrity and is committed to building and strengthening trust with all members of the community. *See* BPD Rule 113 (Public Integrity Policy) and BPD Rule 113A (Bias-Free Policing Policy). All members of the Boston Police Department (sworn and civilian) are committed to providing services and enforcing laws in a professional, nondiscriminatory, fair, and equitable manner. This includes services involving the use of this technology. The Boston Police Department is committed to bias-free policing. *See* BPD Rule 113A (Bias-Free Policing Policy).

The Department is not aware of any finding, outcome, or determination of disparate impact involving this technology.

9. **Agreements: A disclosure of any new agreements made in the past 12 months with non-City entities that may include acquiring, sharing, or otherwise using [the] Surveillance Technology or the Surveillance Data it provides.**

In 2023, the Department did not enter into any new agreements with non-City entities to acquire, share, or utilize the technology to expand the Department's capabilities beyond those that have been previously reported.

Department: Boston Police Department
Surveillance Technology: Crime Laboratory Unit

1. **Description: A description of how [the] Surveillance Technology has been used, including whether it captured images, sound, or other information regarding members of the public who are not suspected of engaging in unlawful conduct.**

The Crime Laboratory Unit utilizes devices, hardware, and software to provide services including:

- Criminalistics
    - Biological screening
    - General evidence examination
    - Crime scene processing including evidence documentation and collection
    - Bloodstain pattern analysis
    - Footwear comparison
    - Firearms
    - Serial number restoration
    - Gunshot residue - distance determination
    - Shooting reconstruction
- DNA
    - Short Tandem Repeat "STR" analysis
    - Combined DNA Index System (CODIS) – Local DNA Index System (LDIS)
- Trace Evidence
    - Hair/fiber examination
    - Unknown materials testing
    - Primer - gunshot residue testing
    - Polymer and glass analysis

CODIS is a software that serves as a computer database that can be used to generate investigative leads through the comparison of DNA profiles. The CODIS database is connected nationwide at the local, state, and national levels, and primarily consists of two indexes, the Forensic Index and the Offender Index. The Forensic Index contains DNA profiles from casework evidence, and the Offender Index contains DNA profiles from convicted offenders and arrestees. The Boston Police Department Crime Laboratory Unit does not maintain any indices containing Offender Samples or other known individuals.

Through the use of computers and high-speed electronic communications technology, the database can rapidly compare the DNA profiles from casework evidence against each other for any possible "hits," or matches. This process is valuable to the identification of serial offenders.

The database can also compare the DNA profiles from casework evidence to the DNA profiles from convicted offenders and other known individuals to potentially identify a suspect in a case that previously was unsolved.

The DNA profiles that Crime Lab contributes to the database consist of casework profiles developed from scene samples from unknown individual(s) if the samples and/or profiles meet certain criteria.

Casework samples are analyzed using a minimum of the 13 core STR loci according to procedures described in the DNA Lab Manual. CODIS Eligible evidence from cases without comparison samples are grouped into two categories, or Batches:

SA: Sexual Assault cases

Other: Homicide, Assault and Battery, Breaking and Entering, Car-Jacking, or any non-sexual assault. "Other" batches can occasionally include Sexual Assaults.

For cases processed in a CODIS Batch or without any known reference samples submitted for comparison, an individual Processing Report will be issued to the investigator in charge of the case containing the results of the DNA analyses. The Processing Reports will indicate whether or not a DNA profile was obtained from an evidence item and whether it is suitable for comparison.

The Processing Report will indicate whether the DNA profile will be entered into CODIS software for searching, the level at which it will be searched (LDIS, SDIS, NDIS), and whether further testing is recommended (e.g. Y-STR testing).

DNA profiles for data entry will be technically reviewed by a second qualified DNA analyst prior to entry. The technical review will confirm the data calls as well as the eligibility of the profile for CODIS entry, using the Technical Review Notes worksheets and the CODIS Entry Worksheet.

All DNA profiles entered into CODIS are searched against a local database of Boston Police Department (BPD) casework profiles for possible case to case hits. Qualifying casework profiles are sent electronically to the Massachusetts State Police (MSP) Crime Laboratory for comparison to casework and known (e.g. convicted offender) profiles from across Massachusetts. Casework specimens with data from 6 (or less than 5 with approval) or more core loci meeting Match Rarity Estimate (MRE) can be uploaded to the MSP. The MSP Crime Lab ultimately sends all of the casework with data from 8 or more of the core loci meeting Match Rarity Estimate (MRE) and known (e.g. convicted offender) profiles from Massachusetts to the FBI for comparison to casework and convicted offender or arrestee profiles from across the United States.

The DNA Section Manual, CODIS Manual, Criminalistics Technical Manual, Quality Manual, Trace Evidence Manual, and CODIS Manual can be provided upon request. The publicly available version of the NDIS Operational Procedures manual can be found at the following link: https://ucr.fbi.gov/lab/biometric-analysis/codis/ndis-procedures-manual

2. **Data Sharing: Whether and how often data acquired through the use of the Surveillance Technology was shared with local, state, and federal [agencies], the name of any recipient entity, the type(s) of data disclosed, any legal standard(s) under which the information was disclosed, and the justification for the disclosure.**

The Crime Lab provides any relevant information as part of its discovery packet to the prosecuting agency for disclosure to criminal defendant(s). Criminal defendants receive surveillance data which is relevant and/or exculpatory to their case through the District Attorney's Office, Attorney General's Office, or United States Attorney's Office pursuant to the rules of discovery, including, but not limited to, Fed. R. Crim. P. 16 and Mass. R. Crim. P. 14, and in accordance with federal and state case law. Additionally, criminal defendants may seek a subpoena or other court order to request the production of specific data

pursuant to the rules of criminal procedure, including, but not limited to, Fed. R. Crim. P. 17 and Mass. R. Crim. P. 17.

Case to case and case to convicted offender/arrestee hits are reported via Hit Notification to the investigator in charge of a case, as well as to the Suffolk County District Attorney's Office. The Hit Notification will contain the identifying information for the case(s), the evidence tested, and the name of the linked individual (if a convicted offender/arrestee or other known hit). Additional information about the convicted offender/arrestee may be listed, such as the social security number or date of birth. This information will vary according to the state jurisdiction that collected the DNA sample from the known offender/arrestee.

A convicted offender/arrestee hit made through CODIS can serve as probable cause to obtain a new DNA sample from the offender/arrestee. The new DNA sample will be processed by the Boston Police Department DNA Section to ensure the accuracy of the DNA match. Upon completion of testing of the new DNA sample from the offender/arrestee, a Comparison DNA Report will be issued to the investigator in charge of the case, as well as the Suffolk County District Attorney's Office, if known.

Data is sent to SDIS (Massachusetts State Police Crime Laboratory) for comparison to casework profiles and convicted offenders from across Massachusetts. Incremental uploads are auto scheduled at a minimum in concordance with the State's searching schedule; uploads can be also sent manually as needed. Full uploads are typically sent as needed, upon notification by SDIS, NDIS or the CODIS Staff (*e.g.*, CODIS Help Desk, etc.).

Data is sent to NDIS for comparison to casework, convicted offender/arrestee, and other known profiles from across the United States. BPD (LDIS) data is sent to NDIS by the MSP (SDIS) only. Samples that meet NDIS acceptance criteria are marked for upload to NDIS at the SDIS level and then forwarded to NDIS for searching. Matches involving BPD data at the NDIS level are automatically sent to the BPD Crime Lab from NDIS and deposited in Match Manager. See "Match Manager from SDIS/NDIS Search" section for details on match disposition and reporting guidelines.

3. Complaints: A summary of community complaints or concerns about the Surveillance Technology, if any.

In an attempt to thoroughly respond to this question, queries were made to the Department's Bureau Chiefs, which includes the Bureau of Field Services, the Bureau of Investigative Services, and the Bureau of Community Engagement, as well as to the individual District Community Service Offices. The Department has not located any specific complaint concerning this technology responsive to this request.

4. Audits: The results of any internal audits, any information about violations of the Surveillance Use Policy, and any actions taken in response other than to the extent that such inclusion would violate the privacy rights of an employee of the City.

Audits: The Crime Laboratory Unit is accredited by ANAB (ISO 17025:2017, AR 3125).
A comprehensive audit was conducted assessing overall operations and work product within the Firearms Analysis Unit (FAU), Latent Print Unit (LPU) and Crime Laboratory Unit (CLU) starting July 7,

2022 and ending November 4, 2022. *See* attached BPD Forensic Division – Audit Report (dated November 17, 2022).

ANAB Audits for the CLU from November 2022 and November 2023 are attached.

Discipline: Compliance with all BPD Policies, Procedures, Rules, SOPs, and Special Orders is monitored by the Bureau of Professional Standards, Internal Affairs Division (IAD). *See* BPD Rule 102 (The Conduct and General Responsibilities of Department Personnel) and BPD Rule 109 (Discipline Procedure).

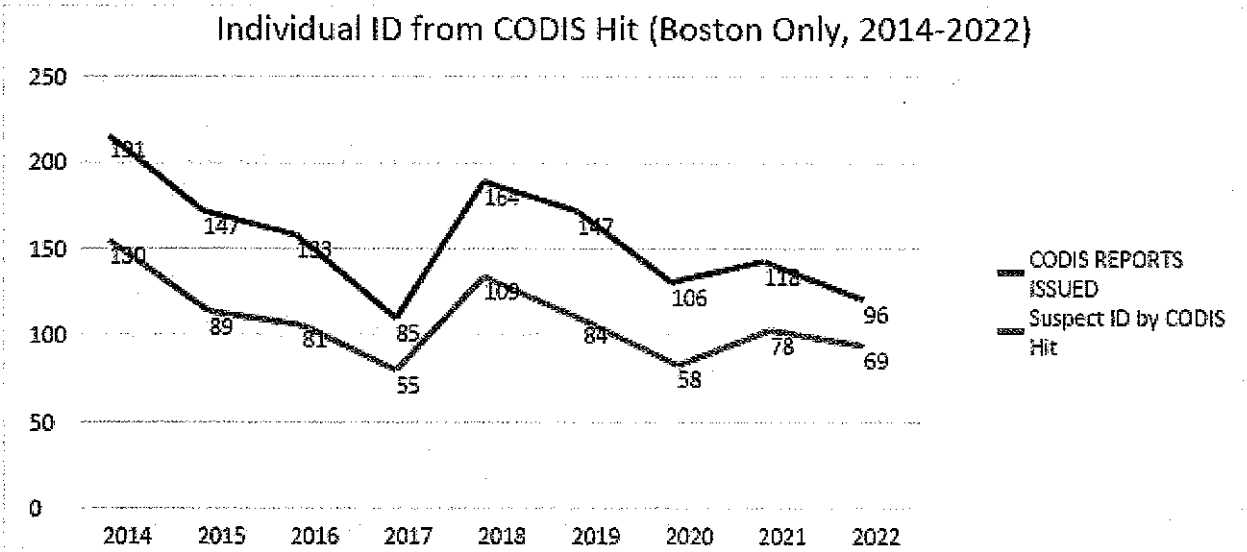
In 2023, there were 0 IAD complaints with an allegation of misuse of the Crime Lab technology or data.

5. Effectiveness: A detailed accounting of whether the Surveillance Technology has been effective at achieving its identified purpose.

Please see attachment regarding the effectiveness of the Department's surveillance technology.

Additionally, in the past nine years, an average of 63% of the CODIS Hits have identified an individual, providing investigative information in the case. (66% in 2021 and 72% in 2022).

In 2022, CODIS Hits generated investigative leads through Case-to-Case Hits or Case-to-Offender/Arrestee Hits for 98 cases. (118 in 2021).



2022 CODIS stats for the CLU:

	Jan	Feb	March	April	May	June	July	Aug	Sept	Oct	Nov	Dec	Total
Profiles entered into CODIS	15	14	14	15	5	2	5	8	11	21	12	9	131
Profiles deleted from CODIS	0	0	0	0	0	0	0	0	0	0	0	0	0
Total profiles in CODIS	4210	4224	4238	4253	4258	4260	4265	4273	4284	4305	4317	4326	
CODIS REPORTS ISSUED	7	12	14	7	5	8	2	4	8	7	21	1	96
Case to Case Hits	5	4	6	3	0	1	0	0	2	2	2	0	25
Case to Offender Hits	4	6	9	5	5	7	3	4	8	5	17	1	74
Suspect ID by CODIS Hit	6	8	10	5	3	7	2	4	7	3	13	1	69

2023 CODIS stats for the CLU:

	Jan	Feb	March	April	May	June	July	Aug	Sept	Oct	Nov	Dec	Total
Profiles entered into CODIS	5	5	15										25
Profiles deleted from CODIS	1	0	2										3
Total profiles in CODIS	4330	4335	4348	4348	4348	4348	4348	4348	4348	4348	4348	4348	
CODIS REPORTS ISSUED	2	6	6										14
Case to Case Hits	1	0	1										2
Case to Offender Hits	1	6	4										11
Suspect ID by CODIS Hit	1	3	2										6

6. Public Records Requests: The number of public records requests received by the City seeking documents concerning Surveillance Technologies approved during the previous year.

The Department received 0 public records requests regarding the CLU.

Public records requests often include a request for any and all information relating to the subject of the request. Due to the broad nature of those requests, the responsive documents could potentially include information relative to this technology. With that in mind, and in order to capture all responsive information to this request, the Department received 5,879 public records requests in 2023. A spreadsheet of all the requests is attached.

7. Cost: An estimate of the total annual costs for the Surveillance Technology, including personnel and other ongoing costs, and what source(s) of funding will fund the technology in the coming year, if known.

Information regarding the Department's FY2023 and FY2024 costs and expenditures is publicly available at: https://www.boston.gov/departments/budget/fy23-operating-budget and https://www.boston.gov/departments/budget/fy24-operating-budget. Information regarding the Department's FY2023 and FY2024 grant funding is attached. The Department's purchases of technology are made through the City of Boston procurement process.

The technology utilized by the CLU does not have any dedicated personnel cost.

8. Impact on Communities: Whether the civil rights and liberties of any communities or groups, including communities of color or other marginalized communities in the City, are disproportionately impacted by the deployment of the Surveillance Technology.

The Boston Police Department strives to maintain the highest standards of honesty and integrity and is committed to building and strengthening trust with all members of the community. *See* BPD Rule 113 (Public Integrity Policy) and BPD Rule 113A (Bias-Free Policing Policy). All members of the Boston Police Department (sworn and civilian) are committed to providing services and enforcing laws in a professional, nondiscriminatory, fair, and equitable manner. This includes services involving the use of this technology. The Boston Police Department is committed to bias-free policing. *See* BPD Rule 113A (Bias-Free Policing Policy).

The Department is not aware of any finding, outcome, or determination of disparate impact involving this technology.

9. Agreements: A disclosure of any new agreements made in the past 12 months with non-City entities that may include acquiring, sharing, or otherwise using [the] Surveillance Technology or the Surveillance Data it provides.

In 2023, the Department did not enter into any new agreements with non-City entities to acquire, share, or utilize the technology to expand the Department's capabilities beyond those that have been previously reported.

Attachments:

(a) BPD Forensic Division Audit Report
(b) ANAB Crime Laboratory Audit Report (Nov. 2022)
(c) ANAB Crime Laboratory Audit Report (Nov. 2023)
(d) Forensic Quality Assurance Standards Audit (June 2023)

Department: Boston Police Department
Surveillance Technology: Latent Print Unit

1. **Description: A description of how [the] Surveillance Technology has been used, including whether it captured images, sound, or other information regarding members of the public who are not suspected of engaging in unlawful conduct.**

The Latent Print Unit (LPU) uses devices, hardware, and software to provide services including:
- Crime scene processing including evidence documentation and collection
- Latent print processing
- Latent print comparison
- Fingerprint Database searches via three AFIS systems

Automated Fingerprint Identification System (AFIS) is a tool used to search unknown latent prints found at crime scenes or recovered from evidentiary items against a database of known fingerprints of individuals. Searches of fingerprints/postmortem prints of unknown deceased individuals is an additional service provided by the LPU. The database provides access to known print records for comparison purposes.

The LPU has access to three AFIS database systems:
- AFIX: local database that contains Boston Police ten print and palm print records. The database was implemented in March 2009 and identifies the candidate list by name.
- MORPHO/Idemia: state database that contains Massachusetts ten print and palm print records. The database was implemented in June 2013 and identifies the candidate list by a State Identification (SID) Number. This database contains both civilian and arrestee records.
- Integrated Automated Fingerprint Identification System (IAFIS)/Next Generation Identification (NGI) (accessed through the state Morpho/Idemia database): federal database that contains federal ten print and palm print records. The database identifies the candidate list by FBI number. This database contains both civilian and arrestee records.

AFIS databases may be utilized by the Criminalist to search latent prints when one or more of the following criteria is met:
- No suspect(s) information is available
- Elimination exemplar prints are provided, and no identifications are made
- A request is made by the Investigator
- Criminalist discretion

A Criminalist (original or verifier) may also utilize AFIS databases to assist in a closed search of a latent print(s) with a subject or multiple subjects. When a verifier performs a closed search, the following should be completed:
- Creation of a case in the database to allow for the closed search
- A "V" will be added at the end of the case number when the verifier is performing a closed search
- All information will be entered to create the case with the verifier's own calibrated image

The Criminalist shall have the authorization to perform or not perform database searches on a case-by-case basis taking into consideration the circumstances of the case and the factors listed below.

A friction ridge impression is suitable for a search when any of the following are present:

- A minimum of 6 clear and unique level two details or higher
- A core and/or delta, or recognizable palm area
- Clarity of detail (may include orientation)

Exigent circumstances may allow for searching of suitable friction ridge impressions prior to complete analysis of all friction ridge impressions in a case.

The LPU also maintains an excel spreadsheet that lists all inked major case impressions being stored in the Forensic Division. Cards are filed by name or criminal record number (CR#). These cards are not considered evidence and copies/representations are retained within the case record as documentation.

Standard Operating Procedures Manual, AFIS Workflow, Mideo Workflow, and Quality Manual include additional information on how the Latent Print Unit utilizes the AFIS databases and can be provided upon request.

2. **Data Sharing: Whether and how often data acquired through the use of the Surveillance Technology was shared with local, state, and federal [agencies], the name of any recipient entity, the type(s) of data disclosed, any legal standard(s) under which the information was disclosed, and the justification for the disclosure.**

Signed reports are retained in LIMS and a copy of the completed report is made available to the Investigator(s). The LPU may provide the District Attorney's Office with a copy of an analysis report upon request by the Assistant District Attorney assigned to the case. In some circumstances, upon verification of a hit performed by a trained and qualified Criminalist, a verbal or written notification of the results can be disseminated to the Investigator prior to the final report. This will be documented in the case record.

The LPU provides any relevant information as part of its discovery packet to the prosecuting agency for disclosure to criminal defendant(s). Criminal defendants receive surveillance data which is relevant and/or exculpatory to their case through the District Attorney's Office, Attorney General's Office, or United States Attorney's Office pursuant to the rules of discovery, including, but not limited to, Fed. R. Crim. P. 16 and Mass. R. Crim. P. 14, and in accordance with federal and state case law. Additionally, criminal defendants may seek a subpoena or other court order to request the production of specific data pursuant to the rules of criminal procedure, including, but not limited to, Fed. R. Crim. P. 17 and Mass. R. Crim. P. 17.

3. **Complaints: A summary of community complaints or concerns about the Surveillance Technology, if any.**

In an attempt to thoroughly respond to this question, queries were made to the Department's Bureau Chiefs, which includes the Bureau of Field Services, the Bureau of Investigative Services, and the Bureau of Community Engagement, as well as to the individual District Community Service Offices. The

Department has not located any specific complaint concerning this technology responsive to this request.

4. **Audits: The results of any internal audits, any information about violations of the Surveillance Use Policy, and any actions taken in response other than to the extent that such inclusion would violate the privacy rights of an employee of the City.**

Audits: The laboratories of the Boston Police Department Forensic Division are currently accredited to ISO/IEC 17025:2017 and ANAB 17025:2017 Forensic Science Testing and Calibration Laboratories Accreditation requirements (AR3125).

A comprehensive audit was conducted assessing overall operations and work product within the Firearms Analysis Unit (FAU), Latent Print Unit (LPU) and Crime Laboratory Unit (CLU) starting July 7, 2022 and ending November 4, 2022. *See* attached BPD Forensic Division – Audit Report (dated November 17, 2022).

ANAB Audits for the LPU from November 2022 and November 2023 are attached.

Discipline: Compliance with all BPD Policies, Procedures, Rules, SOPs, and Special Orders is monitored by the Bureau of Professional Standards, Internal Affairs Division. *See* BPD Rule 102 (The Conduct and General Responsibilities of Department Personnel) and BPD Rule 109 (Discipline Procedure).

In 2023, there were 0 IAD complaints with an allegation of misuse of LPU technology.

5. **Effectiveness: A detailed accounting of whether the Surveillance Technology has been effective at achieving its identified purpose.**

Please see attachment regarding the effectiveness of the Department's surveillance technology.

The addition of an AFIS section in the LPU team has been instrumental in utilizing the AFIS databases effectively as reflected in the statistics listed below. The AFIS section has completed a review of all 2016 through 2019 unsolved homicide cases to determine if additional searches could be performed in those cases.

Latents to AFIS (Local, State, Federal):	Jan	Feb	March	April	May	June	July	Aug	Sept	Oct	Nov	Dec	Total
Number of Latents Submitted:	101	101	103	60	112	38	67	76	67	137	34	44	940
Number of Searches:	112	107	110	69	123	44	77	84	71	154	40	50	1041
Number of Cases:	37	30	27	26	35	13	36	36	33	45	19	23	360
Number of ID/Hits:	34	36	25	14	41	24	23	25	19	30	13	8	292
Number of Cases with ID/Hits:	16	16	11	9	17	8	15	19	13	17	7	6	154

6. **Public Records Requests: The number of public records requests received by the City seeking documents concerning Surveillance Technologies approved during the previous year.**

In 2023, the LPU responded to 0 public records requests.

Public records requests often include a request for any and all information relating to the subject of the request. Due to the broad nature of those requests, the responsive documents could potentially include information relative to this technology. With that in mind, and in order to capture all responsive information to this request, the Department received 5,879 public records requests in 2023. A spreadsheet of all the requests is attached.

7. **Cost: An estimate of the total annual costs for the Surveillance Technology, including personnel and other ongoing costs, and what source(s) of funding will fund the technology in the coming year, if known.**

Information regarding the Department's FY2023 and FY2024 costs and expenditures is publicly available at: https://www.boston.gov/departments/budget/fy23-operating-budget and https://www.boston.gov/departments/budget/fy24-operating-budget. Information regarding the Department's FY2023 and FY2024 grant funding is attached. The Department's purchases of surveillance technology are made through the City of Boston procurement process.

The technology utilized by the LPU does not have any dedicated personnel cost.

8. **Impact on Communities: Whether the civil rights and liberties of any communities or groups, including communities of color or other marginalized communities in the City, are disproportionately impacted by the deployment of the Surveillance Technology.**

The Boston Police Department strives to maintain the highest standards of honesty and integrity and is committed to building and strengthening trust with all members of the community. *See* BPD Rule 113 (Public Integrity Policy) and BPD Rule 113A (Bias-Free Policing Policy). All members of the Boston Police Department (sworn and civilian) are committed to providing services and enforcing laws in a professional, nondiscriminatory, fair, and equitable manner. This includes services involving the use of this technology. The Boston Police Department is committed to bias-free policing. *See* BPD Rule 113A (Bias-Free Policing Policy).

The Department is not aware of any finding, outcome, or determination of disparate impact involving this technology.

9. **Agreements: A disclosure of any new agreements made in the past 12 months with non-City entities that may include acquiring, sharing, or otherwise using [the] Surveillance Technology or the Surveillance Data it provides.**

In 2023, the Department did not enter into any new agreements with non-City entities to acquire, share, or utilize the technology to expand the Department's capabilities beyond those that have been previously reported.

Attachments:

(a) BPD Forensic Division Audit Report
(b) ANAB Latent Print Unit Audit Report (Nov. 2022)
(c) ANAB Latent Print Unit Audit Report (Nov. 2023)

Department: Boston Police Department
Surveillance Technology: Firearms Analysis Unit

1. **Description: A description of how [the] Surveillance Technology has been used, including whether it captured images, sound, or other information regarding members of the public who are not suspected of engaging in unlawful conduct.**

The Firearms Analysis Unit (FAU) utilizes devices, hardware, and software to provide services including:

- Crime scene processing including evidence documentation and collection[2]
- Operational/function testing
- Bullet and cartridge casing comparisons
- Ammunition examination
- Firearm characterization
- Determination of class characteristics
- All cases are entered into the National Integrated Ballistics Information Network (NIBIN)[3] and comparison is performed upon request
- ATF E-Trace system

ATF eTrace is an internet-based system that allows participating law enforcement agencies to submit firearm traces to the ATF National Tracing Center (NTC). eTrace allows for the secure exchange of crime gun incident-based data.

By definition, firearms tracing is the systematic tracking of the movement of a firearm recovered by law enforcement officials from its creation by the manufacturer or its introduction into U.S. commerce by the importer through the distribution chain (wholesaler/retailer) to the first retail purchase. Recovered firearms are traced by Law Enforcement Agencies (a) to link a suspect to a firearm in a criminal investigation; (b) to identify potential firearms traffickers, whether licensed or unlicensed sellers, and; (c) to detect in-state, interstate, and international patterns in the sources and kinds of gun crimes.

Information obtained through the tracing process is utilized to solve and/or enhance individual cases and to maximize investigative lead development through eTrace.

Registered eTrace users can also generate various statistical reports regarding the number of traces submitted over time, the top firearms traced, the average time-to-crime rates, and more. These reports provide a snapshot view of potential firearm trafficking indicators.

The data consists of firearms trace requests, firearms trace results, purchaser, possessor, associate, vehicle and recovery information is captured. This can include an individual's date of birth, place of birth, name, address, height, weight sex, vehicle ID information, driver's license information, recovery

---

[2] FAU uses BEAST (Bar Coded Evidence Analysis Statistics and Tracking) software program which provides Forensic Laboratory Information Management Systems (LIMS) for case management and tracking. The system is included within the Department's list of "Software."

[3] NIBIN and Integrated Ballistics Identification System (IBIS) are used to match ballistic evidence with other cases. Data uploaded to these systems includes test fires with firearms information; no information is identified with an individual.

information, firearms description, Federal Firearms Licensee information, requesting agency information, officer name and contact information, and special instructions.

2. **Data Sharing: Whether and how often data acquired through the use of the Surveillance Technology was shared with local, state, and federal [agencies], the name of any recipient entity, the type(s) of data disclosed, any legal standard(s) under which the information was disclosed, and the justification for the disclosure.**

FAU examiners enter information about seized firearms into the eTrace database. ATF may only disseminate firearm trace related data to a Federal, State, local, tribal, or foreign law enforcement agency, or a Federal, State, or local prosecutor, solely in connection with and for use in a criminal investigation or prosecution; or a Federal agency for a national security or intelligence purpose.

FAU provides any relevant eTrace report(s) as part of its discovery packet to the prosecuting agency for disclosure to criminal defendant(s). Criminal defendants receive surveillance data which is relevant and/or exculpatory to their case through the District Attorney's Office, Attorney General's Office, or United States Attorney's Office pursuant to the rules of discovery, including, but not limited to, Fed. R. Crim. P. 16 and Mass. R. Crim. P. 14, and in accordance with federal and state case law. Additionally, criminal defendants may seek a subpoena or other court order to request the production of specific data pursuant to the rules of criminal procedure, including, but not limited to, Fed. R. Crim. P. 17 and Mass. R. Crim. P. 17.

3. **Complaints: A summary of community complaints or concerns about the Surveillance Technology, if any.**

In an attempt to thoroughly respond to this question, queries were made to the Department's Bureau Chiefs, which includes the Bureau of Field Services, the Bureau of Investigative Services, and the Bureau of Community Engagement, as well as to the individual District Community Service Offices. The Department has not located any specific complaint concerning this technology responsive to this request.

4. **Audits: The results of any internal audits, any information about violations of the Surveillance Use Policy, and any actions taken in response other than to the extent that such inclusion would violate the privacy rights of an employee of the City.**

Audits: The Firearms Analysis Unit is accredited by ANAB (ISO 17025:2017, AR 3125).

A comprehensive audit was conducted assessing overall operations and work product within the Firearms Analysis Unit (FAU), Latent Print Unit (LPU) and Crime Laboratory Unit (CLU) starting July 7, 2022 and ending November 4, 2022. *See* attached BPD Forensic Division – Audit Report (dated November 17, 2022).

Internal Audits: Management reviews are conducted annually in the Firearms Analysis Unit. At the advisement of previous assessment teams, the outcomes of management reviews are forwarded to the Command Staff. Internal unit-wide audits are conducted annually in the Firearms Analysis Unit.

External Audits: Full assessment every four years in the accredited units. Surveillance audits every year, with the exception of full assessment years.

eTrace Auditing: The auditing is accomplished on the Oracle database recording the information activity within the database. Audit trails are designed and implemented to record appropriate information that can assist in intrusion detection. Audit trails are also used as online tools to help identify problems other than intrusions as they occur.

Discipline: Compliance with all BPD Policies, Procedures, Rules, SOPs, and Special Orders is monitored by the Bureau of Professional Standards, Internal Affairs Division. *See* BPD Rule 102 (The Conduct and General Responsibilities of Department Personnel) and BPD Rule 109 (Discipline Procedure).

In 2023, there were 0 IAD complaints with an allegation of misuse of firearms analysis unit technology.

5. **Effectiveness: A detailed accounting of whether the Surveillance Technology has been effective at achieving its identified purpose.**

Please see attachment regarding the effectiveness of the Department's surveillance technology.

6. **Public Records Requests: The number of public records requests received by the City seeking documents concerning Surveillance Technologies approved during the previous year.**

Public records requests often include a request for any and all information relating to the subject of the request. Due to the broad nature of those requests, the responsive documents could potentially include information relative to this technology. With that in mind, and in order to capture all responsive information to this request, the Department received 5,879 public records requests in 2023. A spreadsheet of all the requests is attached.

7. **Cost: An estimate of the total annual costs for the Surveillance Technology, including personnel and other ongoing costs, and what source(s) of funding will fund the technology in the coming year, if known.**

Information regarding the Department's FY2023 and FY2024 costs and expenditures is publicly available at: https://www.boston.gov/departments/budget/fy23-operating-budget and https://www.boston.gov/departments/budget/fy24-operating-budget. Information regarding the Department's FY2023 and FY2024 grant funding is attached. The Department's purchases of technology are made through the City of Boston procurement process.

The technology utilized by the FAU does not have any dedicated personnel cost.

8. **Impact on Communities: Whether the civil rights and liberties of any communities or groups, including communities of color or other marginalized communities in the City, are disproportionately impacted by the deployment of the Surveillance Technology.**

The Boston Police Department strives to maintain the highest standards of honesty and integrity and is committed to building and strengthening trust with all members of the community. *See* BPD Rule 113 (Public Integrity Policy) and BPD Rule 113A (Bias-Free Policing Policy). All members of the Boston Police

Department (sworn and civilian) are committed to providing services and enforcing laws in a professional, nondiscriminatory, fair, and equitable manner. This includes services involving the use of this technology. The Boston Police Department is committed to bias-free policing. *See* BPD Rule 113A (Bias-Free Policing Policy).

The Department is not aware of any finding, outcome, or determination of disparate impact involving this technology.

9. **Agreements: A disclosure of any new agreements made in the past 12 months with non-City entities that may include acquiring, sharing, or otherwise using [the] Surveillance Technology or the Surveillance Data it provides.**

In 2023, the Department did not enter into any new agreements with non-City entities to acquire, share, or utilize the technology to expand the Department's capabilities beyond those that have been previously reported.

Attachments:

(a) BPD Forensic Division Audit Report
(b) ANAB Firearms Analysis Unit Audit Report (Nov. 2023)

Department: Boston Police Department
Surveillance Technology: Software and Databases

1. **Description: A description of how [the] Surveillance Technology has been used, including whether it captured images, sound, or other information regarding members of the public who are not suspected of engaging in unlawful conduct.**

All Boston Police Department personnel utilize software and databases in the course and scope of their employment to support the administrative and investigatory functions of the Department. Software and databases are used only for valid law enforcement purposes, including, but not limited to, enhanced officer awareness, suspect identification, witness and victim identification, resource deployment, investigative support, and to aid in the prosecution of crimes. Additional software and databases are used to support the Department's community service and community caretaking responsibilities.

A detailed, but non-exhaustive, list of software and databases is attached with additional information regarding the data available within the database. This list includes databases maintained by the Department, databases to which the Department contributes data, and databases the Department accesses to view data. The Department also accesses information from publicly available sources, such as social media platforms, including, but not limited to, Facebook, Twitter, Instagram, and SnapChat, and utilizes publicly available applications to improve efficiency in reviewing such information.

2. **Data Sharing: Whether and how often data acquired through the use of the Surveillance Technology was shared with local, state, and federal [agencies], the name of any recipient entity, the type(s) of data disclosed, any legal standard(s) under which the information was disclosed, and the justification for the disclosure.**

All requests made from other law enforcement agencies are handled in accordance with all relevant federal and state laws, BPD rules and regulations, including, but not limited to Special Order 21-46 (Outside Agency Notification), and local ordinances including, but not limited to, Chapter 11-1.9 of the City of Boston Municipal Code (Boston Trust Act).

Criminal defendants receive data which is relevant and/or exculpatory to their case through the District Attorney's Office, Attorney General's Office, or United States Attorney's Office pursuant to the rules of discovery, including, but not limited to, Fed. R. Crim. P. 16 and Mass. R. Crim. P. 14, and in accordance with federal and state case law. Additionally, criminal defendants may seek a subpoena or other court order to request the production of specific data pursuant to the rules of criminal procedure, including, but not limited to, Fed. R. Crim. P. 17 and Mass. R. Crim. P. 17.

3. **Complaints: A summary of community complaints or concerns about the Surveillance Technology, if any.**

In an attempt to thoroughly respond to this question, queries were made to the Department's Bureau Chiefs, which includes the Bureau of Field Services, the Bureau of Investigative Services, and the Bureau of Community Engagement, as well as to the individual District Community Service Offices. In 2023, the Department did not receive any complaints from the community regarding software or databases.

The Department is cognizant that there has been general discussion surrounding the use of technology in the City in various forums and that such discussion may have included complaints or concerns; however, these discussions often occur in forums outside of the Department.

For databases maintained by the BRIC, the BRIC's Privacy Officer, on behalf of the Privacy Committee, is responsible for receiving and responding to inquiries and complaints about privacy, civil rights, and civil liberties protections in the information system(s) maintained or accessed by the BRIC, including the Gang Assessment Database. Complaints and requests for redress are governed by the BRIC Privacy Policy, Section K. In 2023, the BRIC responded to 5 redress requests regarding the Gang Assessment Database.

4. **Audits: The results of any internal audits, any information about violations of the Surveillance Use Policy, and any actions taken in response other than to the extent that such inclusion would violate the privacy rights of an employee of the City.**

Audits: The Department will ensure use of software and databases is in compliance with all applicable laws and regulations. When software or databases have embedded audit features, the Department shall conduct audits as it deems necessary to ensure appropriate use.

The BRIC maintains an audit trail of accessed, requested, or disseminated information. An audit trail will be kept for not more than five (5) years of requests for access to information for specific purposes and of what information is disseminated to each person in response to the request.

Discipline: Compliance with all BPD Policies, Procedures, Rules, SOPs, and Special Orders is monitored by the Bureau of Professional Standards. *See* BPD Rule 102 (The Conduct and General Responsibilities of Department Personnel) and BPD Rule 109 (Discipline Procedure).

In 2023, there were 0 IAD complaints with an allegation of misuse of Department software or databases.

5. **Effectiveness: A detailed accounting of whether the Surveillance Technology has been effective at achieving its identified purpose.**

All Boston Police Department personnel utilize software and databases in the course and scope of their employment to support the administrative and investigatory functions of the Department. Software and databases are used only for valid law enforcement purposes, including, but not limited to, enhanced officer awareness, suspect identification, witness and victim identification, resource deployment, investigative support, and to aid in the prosecution of crimes. Additional software and databases are used to support the Department's community service and community caretaking responsibilities.

Please see attachment regarding the effectiveness of the Department's surveillance technology.

6. **Public Records Requests: The number of public records requests received by the City seeking documents concerning Surveillance Technologies approved during the previous year.**

Public records requests often include a request for any and all information relating to the subject of the request. Due to the broad nature of those requests, the responsive documents could potentially include information relative to this technology. With that in mind, and in order to capture all responsive

information to this request, the Department received 5,879 public records requests in 2023. A spreadsheet of all the requests is attached.

7. **Cost: An estimate of the total annual costs for the Surveillance Technology, including personnel and other ongoing costs, and what source(s) of funding will fund the technology in the coming year, if known.**

Information regarding the Department's FY2023 and FY2024 costs and expenditures is publicly available at: https://www.boston.gov/departments/budget/fy23-operating-budget and https://www.boston.gov/departments/budget/fy24-operating-budget. Information regarding the Department's FY2023 and FY2024 grant funding is attached. The Department's purchases of technology are made through the City of Boston procurement process.

The Department does not have any dedicated personnel cost for this technology.

8. **Impact on Communities: Whether the civil rights and liberties of any communities or groups, including communities of color or other marginalized communities in the City, are disproportionately impacted by the deployment of the Surveillance Technology.**

The Boston Police Department strives to maintain the highest standards of honesty and integrity and is committed to building and strengthening trust with all members of the community. *See* BPD Rule 113 (Public Integrity Policy) and BPD Rule 113A (Bias-Free Policing Policy). All members of the Boston Police Department (sworn and civilian) are committed to providing services and enforcing laws in a professional, nondiscriminatory, fair, and equitable manner. This includes services involving the use of this technology. The Boston Police Department is committed to bias-free policing. *See* BPD Rule 113A (Bias-Free Policing Policy).

The Department is not aware of any finding, outcome, or determination of disparate impact involving this technology.

9. **Agreements: A disclosure of any new agreements made in the past 12 months with non-City entities that may include acquiring, sharing, or otherwise using [the] Surveillance Technology or the Surveillance Data it provides.**

A detailed, but non-exhaustive, list of software and databases the Department utilized in 2023, is attached with additional information regarding the data available within the database.

Software and databases the Department acquired in 2023 include: Asana, Axon Auto Tagging, Axon Interview, First Alert for Public Sector (30-day use only), NIBIN Enforcement Support System (NESS), SAKI Tracking Database System aka "Breadcrumbs," SITE Intelligence Group "SourceFeed" and "SearchFeed" applications (30-day use only), and TRM Forensics-Pro (one year trial). Additionally, FinCEN Query was not acquired in 2023, but was inadvertently omitted from the initial list of software and databases provided by the Department.

Attachments:

(a) List of Software and Databases

Department: Boston Police Department
Surveillance Technology: Gang Assessment Database

1. **Description: A description of how [the] Surveillance Technology has been used, including whether it captured images, sound, or other information regarding members of the public who are not suspected of engaging in unlawful conduct.**

The Gang Assessment Database is used to:

1. Provide law enforcement a consistent citywide framework for identifying individuals and groups that associate as a "gang" and thus are likely to engage in or perpetrate criminal activity for the furtherance of the criminal organization, which may include targeted and/or retaliatory violence.
2. Assist in the investigation of gang related criminal activity in the City of Boston.
3. Assist in identifying at-risk individuals for connection with services.

The Gang Assessment Database does not capture images, sound, or other information regarding members of the public who are not suspected of engaging in unlawful conduct.

Overall, 70% of individuals in the database have a prior firearm related arrest in Boston.

Gang Database victim, offender and criminal history statistics:

- Approximately one quarter of one percent (0.25%) of the City's population is represented in the Database.
- Approximately 32% of the individuals arrested for firearms offenses in 2023 were in the Database.
- Approximately 30% of individuals arrested for shootings in 2023 were in the Database.
- Over the last 5 years, an average of 35% of shootings victims were in the Database.
- 96% of the individuals in the Database have been arrested for a criminal offense in Boston.
- 98% of the individuals in the Database have a criminal history in or outside of Boston.

Following the revision to BPD Rule 335 (Gang Assessment Database, dated July 8, 2021), 2,365 people have been deleted from the Database through 2/15/24.

- In 2023, 111 individuals were added to the Database; 161 individuals were purged from the Database.
- In 2022, 167 individuals were added to the Database; 1,836 individuals were purged from the Database.
- In 2021, 59 individuals were added to the Database; 609 individuals were purged from the Database.
- This info is posted publicly here: https://police.boston.gov/bpd-rule-335-annual-report

Boston Police Department Rule 335 (Gang Assessment Database) with revisions implemented by Special Order 21-27, dated June 8, 2021, and the Boston Regional Intelligence Center (BRIC) Privacy, Civil Rights, and Civil Liberties Protection Policy (2021), govern use of the Gang Assessment Database.

The Database includes Gang Associates and Gangs in accordance with BPD Rule 335. The BRIC maintains copies of supporting documentation for all criteria used to verify an individual. The BRIC analyzes the

validity of the supporting documentation for each individual criteria used to verify an associate and maintain the discretion to decline to use the information towards any criterion. The BRIC maintains the discretion to *decline* to enter individuals into the Database who meet the 10 point criteria but are determined to not be engaged in gang-related criminal activity.

2. **Data Sharing: Whether and how often data acquired through the use of the Surveillance Technology was shared with local, state, and federal [agencies], the name of any recipient entity, the type(s) of data disclosed, any legal standard(s) under which the information was disclosed, and the justification for the disclosure.**

The information in the Database is considered Law Enforcement Sensitive and is thereby For Official Use Only. Its use is limited to the law enforcement community to assist in the prevention, investigation, and resolution of criminal activity. The release of this information beyond these restrictions is strictly prohibited and may constitute a violation of BPD Rules and/or G.L. ch. 268A, § 23. In addition, unauthorized or improper disclosure and/or receipt of this information may impact ongoing investigations or improperly disclose witness identity information, and thereby compromise officer safety as well as that of the public. Attached please find a spreadsheet of the requests for information contained in the Database that the BRIC responded to in 2023.

Specific Authorized Users within the BRIC, selected by the Commander of the Bureau of Intelligence and Analysis (BIA) or his/her designee will have access to print Gang Associate profile pages / face sheets for legitimate law enforcement purposes. All printing from the Database shall be logged and the reason and recipient noted. Attached please find the print log for 2023.

3. **Complaints: A summary of community complaints or concerns about the Surveillance Technology, if any.**

The BRIC's Privacy Officer, on behalf of the Privacy Committee, is responsible for receiving and responding to inquiries and complaints about privacy, civil rights, and civil liberties protections in the information system(s) maintained or accessed by the BRIC, including the Gang Assessment Database. Complaints and requests for redress are governed by the BRIC Privacy Policy, Section K.

In 2023, the BRIC responded to 5 redress requests.

4. **Audits: The results of any internal audits, any information about violations of the Surveillance Use Policy, and any actions taken in response other than to the extent that such inclusion would violate the privacy rights of an employee of the City.**

Audits:

Use/Access Audits: The BRIC maintains an audit trail of accessed information from the Gang Assessment Database. An audit trail will be kept for not more than five (5) years of requests for access to information for specific purposes and of what information is disseminated to each person in response to the request.

Database Audits: Following revision to BPD Rule 335 in 2021, the Database underwent audit and review of all existing individuals to ensure compliance with updates to Section 4.2 ("Gang Associate"), Section 5

("Gang Associate Verification"), and all individuals meeting the definition of "Juvenile" in Section 4.12 to ensure compliance with Section 10 ("Juveniles"). Additionally, audit and review was conducted of all existing individuals in the Database to ensure compliance with updates to Section 9 ("Review of Gang Assessment Database Entries"). This included review of all persons who were entered into the Database more than 5 years prior to the present date to determine based on additional information whether they remain in the "Active" status, per the definition in Rule 335, or will be purged from the Database. Audit and review is ongoing for all persons in the Database: all entries in the Database are reviewed at least every 5 years to determine whether they continue to meet the criteria for inclusion under BPD Rule 335, and juveniles who are included in the Database are reviewed every year.

Following the revision to BPD Rule 335, from July 8, 2021 to February 15, 2024, 2,365 people have been deleted from the Database. In 2023, 111 individuals were added to the Database; 161 individuals were deleted from the Database.

Discipline: Compliance with all BPD Policies, Procedures, Rules, SOPs, and Special Orders is monitored by the Bureau of Professional Standards. *See* BPD Rule 102 (The Conduct and General Responsibilities of Department Personnel) and BPD Rule 109 (Discipline Procedure). In 2023, there were 0 IAD complaints with an allegation of misuse of the Gang Assessment Database.

5. Effectiveness: A detailed accounting of whether the Surveillance Technology has been effective at achieving its identified purpose.

Gangs and gang related violence are impacting neighborhoods in Boston. Intelligence driven community policing is the only way to combat this pervasive issue. As the name suggests, this model starts with intelligence. The intelligence and analysis provided by the Boston Regional Intelligence Center is essential in directing department resources and guiding investigations. The Gang Assessment Database is one tool that aids the BRIC in providing analysis to drive operational decision making as well as providing real time information in wake of violent events.. For example:

- In January 2023, officers responded to a radio call for shots fired on Prentiss Street and located a victim suffering from two gunshot wounds. Detectives utilized the BAT Camera System / FLIR to view the suspects who wore masks before and after the shooting. Detectives then utilized residential and commercial video to track the covered-up suspects by their clothing to the area of a housing development. Detectives pulled additional video from Boston Housing Authority and viewed the suspects in the same clothing unmasked. Detectives identified the suspects with these images and the Gang Assessment Database. Thereafter, a search warrant was executed and four (4) firearms were recovered.
- In April 2023, the Gang Assessment Database was utilized to identify an individual in relation to a person shot incident. From an "Identification Wanted" bulletin, a police officer recognized the individual from a report of a gang member who had been arrested approximately one month earlier.
- In August 2023, officers responded to a shooting in the area of Wales Street and Browning Ave in the Dorchester section of Boston. At the time of the shooting, there was an ongoing basketball tournament at a nearby park. Area B3 detectives determined that the shooting involved one individual who was shot multiple times while seated in a vehicle and another individual returned fire at the original shooter. Detectives quickly ascertained the identity of the individual who returned fire, but the original shooter remained at large. Detectives subsequently distributed a

still frame from the incident. Based on open source social media posts and the Gang Assessment Database, officers identified the original shooter and obtained an arrest warrant.

- In August 2023, the J'ouvert Parade was interrupted when three armed gunmen exchanged gunfire and eight victims sustained non-fatal injuries. Immediately following the shooting, the Gang Assessment Database provided officers with information about the individuals involved, including their gang involvement in two groups that have a long-standing feud. BRIC Analysts also reviewed video footage from the BAT Camera System, which along with the associational information provided by the Gang Assessment Database, allowed officers to identify one of the shooters. Three suspects who fired shots were arrested and a fourth suspect was arrested for carrying an illegal firearm. Two firearms were recovered.

The database is only used for valid law enforcement purposes, including enhanced officer awareness, suspect identification, witness and victim identification, resource deployment, investigative support, and to aid in the prosecution of gang related crimes. Additionally, the Database has proven effective in identifying at risk individuals in order to connect them with services

Please see attachment regarding the effectiveness of the Department's surveillance technology for additional information.

6. **Public Records Requests: The number of public records requests received by the City seeking documents concerning Surveillance Technologies approved during the previous year.**

The Department received 3 requests for information specifically regarding the Gang Assessment Database.

In 2023, the Department received 5,879 public records requests, including the 3 requests specifically regarding the Gang Assessment Database. All public records requests the Department received in 2023 are attached.

7. **Cost: An estimate of the total annual costs for the Surveillance Technology, including personnel and other ongoing costs, and what source(s) of funding will fund the technology in the coming year, if known.**

Information regarding the Department's FY2023 and FY2024 costs and expenditures is publicly available at: https://www.boston.gov/departments/budget/fy23-operating-budget and https://www.boston.gov/departments/budget/fy24-operating-budget. Information regarding the Department's FY2023 and FY2024 grant funding is attached. The Department's purchases of technology are made through the City of Boston procurement process.

The Department does not have any dedicated personnel cost for this technology.

8. **Impact on Communities: Whether the civil rights and liberties of any communities or groups, including communities of color or other marginalized communities in the City, are disproportionately impacted by the deployment of the Surveillance Technology.**

The Boston Police Department strives to maintain the highest standards of honesty and integrity and is committed to building and strengthening trust with all members of the community. *See* BPD Rule 113

(Public Integrity Policy) and BPD Rule 113A (Bias-Free Policing Policy). All members of the Boston Police Department (sworn and civilian) are committed to providing services and enforcing laws in a professional, nondiscriminatory, fair, and equitable manner. The Boston Police Department is committed to bias-free policing. BPD Rule 113A (Bias-Free Policing Policy).

The Department maintains that no civil rights and liberties have been impacted as a result of its use of the Gang Assessment Database. The Department recognizes that the Gang Assessment Database has been criticized as a dataset that predominantly contains people of color. This unfortunate disparity is due to the gang dynamics in the City of Boston and not as a result of any racially biased practices.

9. **Agreements: A disclosure of any new agreements made in the past 12 months with non-City entities that may include acquiring, sharing, or otherwise using [the] Surveillance Technology or the Surveillance Data it provides.**

No agreements with non-City entities. The Department entered into a Memorandum of Understanding with the Mayor's Office for Community Safety to facilitate sharing of data and information.

Attachments:

(a) Gang Database Print Log 2023
(b) Gang Database Request for Information 2023
(c) Memorandum of Understanding Between the Boston Police Department and the Mayor's Office for Community Safety

Department: Boston Police Department
Surveillance Technology: Unmanned Aerial Systems (UAS) – Drone Technology

1. **Description: A description of how [the] Surveillance Technology has been used, including whether it captured images, sound, or other information regarding members of the public who are not suspected of engaging in unlawful conduct.**

Remotely operated Unmanned Aerial Systems (UAS) can be effectively utilized to provide first responders with critical information in calls for service, emergency situations, or criminal investigations.

The Boston Police Department Bureau of Field Services, Homeland Security Unit safely and efficiently deploys UAS for legitimate law enforcement purposes, including, but not limited to, the following: providing detailed documentation of crime and crash scenes; assisting in searches for lost or missing children; in support of BPD responses to Code 99 Special Threat Situations, as defined in BPD Rule 200 (Critical Incident Management); and in preparation of large-scale events with significant public safety concerns.

The Bureau of Investigative Services, Crime Scene Response Unit utilizes drones in aerial photography of crime scenes and accident reconstruction.

The Office of the Superintendent-In-Chief, Office of Multi-Media Productions has one UAS that, to date, has not been used. Once the drone is registered, it will be used for public relations and training purposes only. It will not be used for criminal investigations, and it will not be deployed in a manner that allows it to record any personal identifying information.

Additional drone technology includes DJI AeroScope Drone Detection Technology utilized by the Bureau of Intelligence and Analysis, Boston Regional Intelligence Center. The system passively monitors for DJI brand UAS operating in the region and has the ability to set up alerts to detect UAS flight within a geofenced zone, such as an area surrounding critical infrastructure. The system can be actively monitored during large scale, high risk special events, major dignitary visits, or as needed based on threat intelligence. The system provides the geographic coordinates of the UAS (including, height, direction of flight and speed), location of the pilot, and serial number of the drone. No personal identifiable information is collected by the system and a search warrant is required to identify the registered owner of the UAS through the serial number of the UAS. DJI brand UAS owners sign a consent agreement when they register their drones prior to use that authorizes monitoring in this manner.

All Department UAS are equipped with individual cameras that have the ability to record video footage. The video footage is retained in one of two ways. On most flights, the footage is retained on a memory card. If said footage involves a criminal investigation it is transferred, in its entirety, to an external disc or thumb drive. If the flight is recorded through the FLIR Video Management System, it is retained on the FLIR storage system for a period of thirty days.[4]

[4] Flights which are recorded through the FLIR System typically involve emergency situations where it is necessary to provide live feed access to BPD Command elements who are not on scene.

None of the cameras can record audio. The Department has two UAS cameras that have the ability to view and record with thermal capacity capabilities.

All UAS cameras are used to navigate the UAS as a "first person viewing" camera while it is in flight. Pursuant to the Department's Operations Manual regarding "Protection of Privacy," when a UAS is deployed the onboard camera shall be turned to be facing away from all persons and occupied structures, unless the camera needs to be used solely for the purposes of safely navigating the National Air Space, until the UAS reaches the subject of the deployment.

All UAS must be operated at such an altitude, speed, and with a planned flight pattern, that will ensure inadvertent video recordings or photographs of private spaces of third parties are avoided or minimized. If recording is not necessary during part of, or the entirety of the UAS deployment, such as the camera being used solely for navigation purposes, the Department will not record any video information - it will only be live streamed to the pilot.

UAS shall not be intentionally used for viewing, recording, or transmitting images and/or video in a criminal investigation at any location or property where a person has a reasonable expectation of privacy unless a warrant has been approved for the search of the property, exigent circumstances exist, or the owner or person responsible for the property has given their consent.

All Department UAS pilots are required to properly document all Department flights electronically, via either AirData logbook or, if AirData is not compatible with the UAS, with equivalent software.

A spreadsheet of all 2023 drone flights is attached.

2. **Data Sharing: Whether and how often data acquired through the use of the Surveillance Technology was shared with local, state, and federal [agencies], the name of any recipient entity, the type(s) of data disclosed, any legal standard(s) under which the information was disclosed, and the justification for the disclosure.**

In 2023, no information was shared and no information was exchanged when UAS were used in conjunction with city agencies and outside local agencies. Information will only be shared with other City Agencies subject to the approval of the Police Commissioner. If approval is granted, the UAS Manager is responsible for coordinating the release of any information to another City Agency.

All requests made from other law enforcement agencies are handled in accordance with all relevant federal and state laws, BPD rules and regulations, including, but not limited to Special Order 21-46 (Outside Agency Notification), and local ordinances including, but not limited to, Chapter 11-1.9 of the City of Boston Municipal Code (Boston Trust Act).

Criminal defendants receive data which is relevant and/or exculpatory to their case through the District Attorney's Office, Attorney General's Office, or United States Attorney's Office pursuant to the rules of discovery, including, but not limited to, Fed. R. Crim. P. 16 and Mass. R. Crim. P. 14, and in accordance with federal and state case law. Additionally, criminal defendants may seek a subpoena or other court order to request the production of specific data pursuant to the rules of criminal procedure, including, but not limited to, Fed. R. Crim. P. 17 and Mass. R. Crim. P. 17.

3. **Complaints: A summary of community complaints or concerns about the Surveillance Technology, if any.**

In an attempt to thoroughly respond to this question, queries were made to the Department's Bureau Chiefs, which includes the Bureau of Field Services, the Bureau of Investigative Services, and the Bureau of Community Engagement, as well as to the individual District Community Service Offices. The Department has not located any specific complaint concerning this technology responsive to this request.

The Department is cognizant that there has been general discussion surrounding the use of technology in the City in various forums and that such discussion may have included complaints or concerns; however, these discussions often occur in forums outside of the Department and, as a result, the Department has been unable to locate any specific complaints relative to this technology.

4. **Audits: The results of any internal audits, any information about violations of the Surveillance Use Policy, and any actions taken in response other than to the extent that such inclusion would violate the privacy rights of an employee of the City.**

Audits: A spreadsheet of all 2023 drone flights is attached.

The Boston Police Department UAS Manager is responsible for ensuring UAS annual statistics are saved for all UAS deployments; ensuring that all BPD UAS information that is required to be retained by all applicable laws and ordinances is provided to the Office of the Police Commissioner on an annual basis; and ensuring that all flight and training records are properly maintained by all Department UAS pilots.

All Department UAS pilots are required to properly document all Department flights electronically, via either AirData logbook or, if AirData is not compatible with the UAS, with equivalent software. Training flights are also required to be recorded in either AirData logbook or equivalent software if AirData is not available. This information must be logged after each mission and as soon as practicable.

The UAS Manager is tasked with ensuring all recordings or other information that is gathered as a result of the UAS deployment are properly stored in accordance with Department Rules and Procedures.

Discipline: Compliance with all BPD Policies, Procedures, Rules, SOPs, and Special Orders is monitored by the Bureau of Professional Standards, Internal Affairs Division. *See* BPD Rule 102 (The Conduct and General Responsibilities of Department Personnel) and BPD Rule 109 (Discipline Procedure). Any officer that uses UAS without proper authorization, deviates from the standards in BPD Rule 407, or violates any other Department Rules or Procedures may be subject to disciplinary action.

In 2023, there were 0 IAD complaints with an allegation of violation of Rule 407 and 0 IAD complaints with an allegation of misuse of drone technology.

5. **Effectiveness: A detailed accounting of whether the Surveillance Technology has been effective at achieving its identified purpose.**

In 2023, the Department deployed UAS for legitimate law enforcement purposes, including, but not limited to, the following: providing detailed documentation of crime and crash scenes (including aerial photography and video of crime scenes and accident scenes); assisting in searches for lost or missing children; in support of BPD responses to Code 99 Special Threat Situations, as defined in BPD Rule 200 (Critical Incident Management); and in preparation of large-scale events with significant public safety concerns.

For example:

- On July 8, 2023, a drone was deployed during this missing person investigation after detectives received information that the missing person, a young man with Asperger's Syndrome and multiple mental health disorders, frequented a nearby, wooded area. The drone did not locate the young man; however, the search allowed investigators to be confident he was not in that area at that time and to focus efforts elsewhere.
- In March 2023, an 89-year-old male with dementia, kidney, and heart issues, walked away from his home in Mattapan. Investigators deployed a Drone with infrared capabilities to search nearby areas, including footpath of the Neponset River Greenway, the Neponset River riverbank, and railroad tracks. Although the drone did not locate the man, the efficiency and speed of the search by the Drone allowed officers to further expand their search area outward, and the victim was located hours later in the Town of Milton.

Please see attachment regarding the effectiveness of the Department's surveillance technology for additional information.

6. **Public Records Requests: The number of public records requests received by the City seeking documents concerning Surveillance Technologies approved during the previous year.**

The Department received 2 public records requests for information specifically regarding drones.

Public records requests often include a request for any and all information relating to the subject of the request. Due to the broad nature of those requests, the responsive documents could potentially include information relative to this technology. With that in mind, and in order to capture all responsive information to this request, the Department received 5,879 public records requests in 2023, including the two referenced above. A spreadsheet of all the requests is attached.

7. **Cost: An estimate of the total annual costs for the Surveillance Technology, including personnel and other ongoing costs, and what source(s) of funding will fund the technology in the coming year, if known.**

In FY 2023, the Department did not have any expenditures for UAS.

Information regarding the Department's FY2023 and FY2024 costs and expenditures is publicly available at: https://www.boston.gov/departments/budget/fy23-operating-budget and https://www.boston.gov/departments/budget/fy24-operating-budget. Information regarding the

Department's FY2023 and FY2024 grant funding is attached. The Department's purchases of technology are made through the City of Boston procurement process.

The Department does not have any dedicated personnel cost for this technology.

8. **Impact on Communities: Whether the civil rights and liberties of any communities or groups, including communities of color or other marginalized communities in the City, are disproportionately impacted by the deployment of the Surveillance Technology.**

The Boston Police Department strives to maintain the highest standards of honesty and integrity and is committed to building and strengthening trust with all members of the community. *See* BPD Rule 113 (Public Integrity Policy) and BPD Rule 113A (Bias-Free Policing Policy). All members of the Boston Police Department (sworn and civilian) are committed to providing services and enforcing laws in a professional, nondiscriminatory, fair, and equitable manner. This includes services involving the use of this technology. The Boston Police Department is committed to bias-free policing. *See* BPD Rule 113A (Bias-Free Policing Policy).

The Department is not aware of any finding, outcome, or determination of disparate impact involving this technology.

9. **Agreements: A disclosure of any new agreements made in the past 12 months with non-City entities that may include acquiring, sharing, or otherwise using [the] Surveillance Technology or the Surveillance Data it provides.**

In 2023, the Department did not enter into any new agreements with non-City entities to acquire, share, or utilize the technology to expand the Department's capabilities beyond those that have been previously reported.

Attachments:

(a) Spreadsheet of Drone Flights 2023

Department: Boston Police Department
Surveillance Technology: Vehicles Equipped with Surveillance Technology

1. **Description: A description of how [the] Surveillance Technology has been used, including whether it captured images, sound, or other information regarding members of the public who are not suspected of engaging in unlawful conduct.**

The Boston Police Department deploys the following surveillance technology in vehicles:
(1) Cameras, both recording and non-recording
(2) Cell-site simulator

Please see the Annual Surveillance Reports for these technologies.

Supplemental Documents

This publicly-viewable Google Drive Folder contains links for all of the attachments referenced in the above Annual Surveillance Reports.